Checkmarx CxSAST Plugin

Plugin Information
View Checkmarx on the plugin site for more information.

This plugin adds an ability to perform automatic code scan by Checkmarx server and shows results summary and trend in Jenkins interface.

Summary

Checkmarx CxSAST is a unique source code analysis solution that provides tools for identifying, tracking, and repairing technical and logical flaws in the source code, such as security vulnerabilities, compliance issues, and business logic problems.

Without needing to build or compile a software project's source code, CxSAST builds a logical graph of the code's elements and flows. CxSAST then queries this internal code graph. CxSAST comes with an extensive list of hundreds of preconfigured queries for known security vulnerabilities for each programming language. Using the CxSAST Auditor tool, you can configure your own additional queries for security, QA, and business logic purposes.

CxSAST provides scan results either as static reports, or in an interactive interface that enables tracking runtime behavior per vulnerability through the code, and provides tools and guidelines for remediation. Results can be customized to eliminate false positives, and various types of workflow metadata can be added to each result instance. These metadata are maintained through subsequent scans, as long as the instance continues to be found.

The input to CxSAST's scanning and analysis is the source code, not binaries, so no building or compiling is required, and no libraries need to be available. The code doesn't even need to be able to compile and link properly. Consequently, CxSAST can run scans and generate security reports at any given point in a software project's development life cycle.

The CxSAST Jenkins plugin enables:

- Automatic code scan on CxSAST server, upon each build triggered by Jenkins
- Ability to run Open Source Analysis (CxOSA) from within Jenkins
- Graphical Scan results summary and trends in Jenkins interface
- Links from Jenkins to CxSAST and CxOSA detailed scan results and to PDF report

After setting up the plugin, you can configure any Jenkins job with a build step action to activate a CxSAST scan. When a Job scan (build) is activated, Jenkins sends the job's source code to CxSAST, where it is scanned according to the parameters specified in the build step action. The scan results are stored in the CxSAST project specified in the action, and displayed in the Jenkins job.

CxOSA for Jenkins can be run in cases where open source components are used as part of the development effort. When a CxOSA (build) is activated, Jenkins sends the open source fingerprints to the CxOSA service (note that no customer details or used libraries are passed to the CxOSA service). Using these open source fingerprints, the CxOSA service maps the open source libraries, identifies the vulnerabilities, analyses license risk and compliance, builds the inventory and detects outdated libraries. Comprehensive and summarized reports are generated within the Jenkins interface.

For release notes see:

- CxSAST Release Notes

For more information see:

- CxSAST Jenkins Plugin