



CHECKMARX
choose what developers use

Checkmarx CxSAST v8.2.0 Release Notes

September, 2016

8.2.0 Release Updates

CxSAST 8.2.0 includes the following updates:

New Features and Changes

Application

Category	Features
Licensing	<p>A new licensing structure has been implemented into this new version of CxSAST</p> <ul style="list-style-type: none"> • Choice of two product editions - SDLC (for developers) and Security Gate (for AppSec champions) • Number of projects • Number of users <ul style="list-style-type: none"> ○ Users (combined roles) ○ Auditor Users • Number of concurrent scans (formerly engines) • Additional licensing, for example, Open Source feature enablement <p>Contact your Checkmarx sales representative for more information.</p>
Setup	<p>A new installation wizard has been implemented into the CxSAST application setup reducing the time and complexity of the installation procedure. The setup interface has been completely re-designed and includes two installation types for standard users and advanced users.</p>
Project State - CxOSA	<p>A new process indicator has been added to the Open Source Analysis procedure (Dashboard > Project State > View Analysis Results > CxOSA) in cases where the user activates the PDF download action. Once activated, the process indicator reads “Open Source Analysis Report download PDF is in progress”.</p>
Project State - CxOSA	<p>A new vulnerability score indicator has been added to the Open Source Analysis status (Dashboard > Project State > View Analysis Results > CxOSA). In combination with the existing color scale, the status indicator now displays the “Vulnerability Score: High (as Red), Medium (as Orange) or Low (as Yellow)”.</p>

Category	Features
Checkmarx Academy - AppSec Coach	<p>In parallel with the Checkmarx Academy this new version of CxSAST provides collaborative integration with the highly interactive and intuitive Application Security Training platform (AppSec Coach™). This helps developers learn by interacting with real vulnerable applications and the underlying code-behind.</p> <p>This version includes a free edition of AppSec Coach™ and covers 3 lessons (SQL Injection (SQLi), Cross-site scripting (XSS), XML Injection (XXE)) and 6 languages (Java, .Net, PHP, Node.JS, Ruby, Python).</p> <p>The full and paid version is expected for future versions and will include 100+ lessons and additional languages.</p>
Scan Results	<p>Interactive links to the AppSec Coach from within the CxSAST application are positioned in the following locations; Scan Results Viewer (Dashboard > Project State > Open Viewer) and the Query Description Viewer (Scan Results Viewer > Scan Results pane > Query Name > ?)</p>
Dashboard	<p>A new product edition indicator has been added to the CxSAST System Dashboard and is positioned next to the Checkmarx logo/version. This indicator specifies the type of product edition currently installed (SDLC or Security Gate).</p>
Management - Application Settings	<p>A new product edition indicator (Edition) has been added to the General panel in the License Details screen (Management > Application Settings > License Details > General). This indicator specifies the type of product edition currently installed (SDLC or Security Gate).</p>
Management - Application Settings	<p>A new panel (Capacity) has been added to the License Details screen (Management > Application Settings > License Details > Capacity). The main areas of interest are number of users, auditor users, projects and engines (in use and available).</p> <p>This new panel replaces the Roles, Companies and Service Providers panels in previous versions.</p>
Management - Application Settings	<p>A new panel (License Expiration Notification) has been added to the License Details screen (Management > Application Settings > License Details > License Expiration Notification). This panel contains the Notification by E-mail parameter. If checked, a notification email is automatically sent to the CxSAST Administrator User on a weekly basis starting 90 days (defined in the DB) before the actual license is set to expire.</p>

Category	Features
Management - Scan Settings	<p>An updated version of the default preset (Checkmarx Default) has been added to the list of Presets in the Preset Manager screen (Management > Scan Settings > Preset Manager > Preset List > Checkmarx Default). This new preset essentially contains all the vulnerabilities that Checkmarx recommends to scan in cases when you are unsure about which preset to use.</p> <p>This preset will eventually replace the existing Default and Default 2014 presets.</p>
Management - Scan Settings	<p>A new preset (OWASP Mobile Top 10) has been added to the list of Presets in the Preset Manager screen (Management > Scan Settings > Preset Manager > Preset List > Checkmarx Default). This essentially contains all the vulnerabilities for mobile application security risks in accordance with OWASP Mobile Top 10 compliance guidelines for 2016.</p>

Integration & Plugins

Category	Features
IntelliJ – Scan Results	<p>In parallel with the Checkmarx Academy the new version of IntelliJ plugin for CxSAST (8.2.0) provides collaborative integration with a highly interactive and intuitive Application Security Training platform (AppSec Coach) that helps developers learn by interacting with real vulnerable applications and the underlying code-behind.</p>
IntelliJ – Scan Results	<p>Interactive links to the AppSec Coach from within the IntelliJ are positioned in the following locations; Scan Results Viewer (Dashboard > Project State > Open Viewer) and the Query Description Viewer (Scan Results Viewer > Scan Results pane > Query Name > ?)</p>
Integration - Jenkins	<p>The Jenkins plugin for CxSAST (v8.2.0) has been upgraded and now supports Jenkins version 2.7. As for the limitation for previous versions there is now no need to install the Maven Plugin in order for our Jenkins Plugin to work.</p>

Category	Features
Integration - Jenkins	A new checkbox (Avoid duplicate project scans in queue) has been added to this new version of CxSAST Plugin for Jenkins (Job > Configure > Build > Add Build Step > Execute Checkmarx Scan > Scan Action Configuration). This new checkbox option, if activated, ensures that if a build is initiated in Jenkins and there is already a scan request for this project in the CxSAST Queue, then do not send another scan request. Note that Open Source Analysis will also not be activated in this case.

Engine

Category	Features
Supported Languages	Informix ESQLC language support - extended provision for the C language by adding support for the Embedded SQL Framework which enables direct access from C source code to IBM databases. Informix ESQLC is being introduced via open beta.
Logs	Enhanced scan engine log files provide users, support and professional service team's additional information to understand and troubleshoot Engine behavior. Old style log files will be kept until the new ones are in full use.
Vulnerability Descriptions	New vulnerability descriptions – updated vulnerability descriptions giving more detailed guidance for code remediation
Scan Improvements	Major advances in the engine providing significant reduction in false positives and false negatives across all supported languages

Resolved Issues

Category	Resolved Issues
Application	Improvements and fixes in the CxSAST installation/upgrade process
Application	Improvements in correlation results between the reporting and compare scan
Application	Fixed export CSV file issue for compare scan option
Application	Fixed Sort/Group By issues in the Queue Window



Category	Resolved Issues
Visual Studio Plugin	Fixed scanning of multiple files issue in Visual Studio plugin
Jenkins Plugin	Fixed Comments option in Jenkins plugin
Perforce Integration	Improvements and fixes with User Permissions/Directory issues for Perforce integration
JIRA Integration	Fixed ticketing issues for JIRA integration
Engine	Improvements and fixes for the following languages: <ul style="list-style-type: none"> • Apex • Java • PL/SQL • JavaScript • PHP • ObjectiveC • C# • CCP • Ruby • VbNet

Known Limitations

Category	Known Limitations
Setup - Uninstall	During uninstall of the CxSAST application, in cases when the CxWeb site was created on IIS, the CxWeb may not be removed. This does not interfere with the uninstall process but, if required, it can be removed manually from the IIS Manager.
CxAudit - Licensing	When auditing or performing a scan in CxAudit and the timeout threshold passes, the audit user is requested to login again. If the login fails due to licensing issues, request from your system administrator to release the license and try to login again. Note that, if you click Cancel, CxAudit will close and any running scans and results will be deleted.