Checkmarx CxSAST

Release Notes for 8.4.2 (GA Release)

April, 2017

Contents

New Features and Changes

Application

Category	Features
LDAP Authentication / Synchronization	In this version of CxSAST the LDAP Synchronization (User Authorization Management) feature has been enhanced to support the definition of LDAP users to be mapped to specific Viewer/ Scanner with attributes (e.g. assign group to "Scanner without any Authorities" or assign group to "Reviewer with Not Exploitable" options).
	CxSAST now provides the ability for the user to login via the SSO. This means that the SSO users is automatically created upon a successful SSO Login (instead of the current need to create the user in advance). This can be enabled from the LDAP configuration screen (Management > Connection Settings > LDAP Servers > Enable SSO).
Integration – CxOSA	The enable/disable option has been removed from CxSAST and as in previous versions CxSAST still supports the option to perform open source analysis to locally stored as well as shared directory folders and files. This means that CxOSA is now enabled by default.
	The following file extensions have been added for WhiteSource in this version of CxOSA: nupkg, plx, pm, ph, cgi, fcgi, psgi, al, perl, t, p6m, p6l, nqp, 6pl, 6pm, p6.
	Improvements in the CxOSA-WS Activation Utility.
Projects & Scans	A new configuration option (multi-language scan) has been added to the creating and configuring a CxSAST project process. Configuration selection is traditionally for advanced users only and now provides the possibility to select a multi-language configuration. The file threshold parameter is set to 0 by default and means that all files will be scanned in case of multi-language selection. If there is a need this parameter can be adjusted in the database.
Management - AppSec Coach Statistics	AppSec Coach™ is an in-context eLearning platform that sharpens the skills developers need to fix vulnerabilities and write secure code. The AppSec Coach Statistics Dashboard provides the Checkmarx administrator with the capability to perform ongoing analysis on running AppSec Coach programs, therefore providing information about the progress of participating users and the types of courses and modules being taken.

Audit

Category	Features
CxAudit Workspace	A new Edit Queries menu has been added to the Audit Workspace screen. This provides the capability to add a query to the Audit View without loading a project. Click the Edit Queries menu on the Audit Workspace, select the relevant language from the drop-down and click Edit Queries. An empty query file is created with the extension relevant to the language selected.
	The Refresh menu option on the Audit Workspace is now available for non-admin users as well as admin users.
	When creating a New Local Project in the Audit Workspace and selecting the Project Directory drop-down, CxAudit now displays a list of the last five (5) projects.
	The scans for each project in the Audit Workspace are now sorted by date and not alphabetically. This makes it easier for the user to define which scan was the first scan and which one is the latest.
Audit View	AppSec Coach™ has been added to the CxAudit adding a whole new look and feel to the Auditor. This option can be accessed by right-clicking on a query and selecting Show Description. Clicking (Checkmarx Knowledge Center > 8.4.2 Release Updates > image2017-2-22_16-46-51.png) takes you to the AppSec Coach. This version still includes a free edition of AppSec Coach™ that covers 3 lessons (SQL Injection (SQLi), Cross-site scripting (XSS), XML Injection (XXE) and 6 coding languages (Java, .Net, PHP, Node.JS, Ruby, Python). The full and paid version will include 100+ lessons and additional coding languages.
	CxAudit now provides the capability to control the arrow functionality in the Audit View using keyboard shortcuts (Ctrl + left/right arrows).
	CxAudit now provides the capability to increase/decrease the font size of the code in the Source Code panel for the Audit View. This can be achieved, while in Audit View, by using the + - magnifier icons on the toolbar.
	CxAudit now provides the capability to edit code for a project from the Source Code panel in the Audit View. You can simply right-click on the code in the Source Code panel, select the Edit option and edit the code in the default text editor that appears.

Category	Features
	When editing a query in the Query Source panel in the Audit View, CxAudit now provides the capability to open the Atomic Query API Guide. Right-click on the query code in the Query Source panel and select the Atomic Query API Guide option. The relevant version of the Atomic Query API Guide (.pdf) is displayed.
	A new menu option (Audit View > Source Code panel > right-click element > Find Definition) has been included in this version of CxAudit. This provides the capability to find the definition of a certain element in the Source Code panel. Once selected, the results are displayed in the Results panel. Clicking on one of the results in the Result panel takes you to the definition in the Source Code panel.
	A new menu option (Audit View > Source Code panel > right-click element > Find All References) has been included in this version of CxAudit. This provides the capability to find any references to a certain element in the Source Code panel. Once selected, any results are displayed in the Results panel. Clicking on one of the results in the Result panel takes you to the reference in the Source Code panel.
	CxAudit now provides the capability to quickly navigate to the source code in the Query Source panel. This is achieved by double-clicking on the query in the Query Results History (Results panel).
File and Folder Location	Previous to this new version, CxAudit could only be accessed by an administrator user. In order to allow CxAudit to be run by non-administrator users, we moved the files and folders that were created during the CxAudit and CxEngine run. These files and folder have been moved from the Program Folder to the User's AppData folder and Window's Temporary folder. These files include Logs, Logs/Analytics, PersistentState, Temporary files used to calculate disk speed, Config.xml, DefaultConfig.xml, JsRunnerMapping.pid, FileExtension.xml, locking.cx, History, CxAuditSrc. In addition, CxAudit temporary ZIP files received on the network and extracted, have been moved to Window's temporary folder. Note that CxEngine files are moved only if the CxEngine is executed from the CxAudit. In all other cases these files remain in their original locations.
Open Logs and Config Folder	In order to accommodate the file location changes, a new menu item (File > Open Logs and Config Folder) has been created in order to provide easy access to the logs and defaultConfig.xml files.

Integration & Plugins

Category	Features
IDE – Visual Studio	AppSec Coach™ has been added to the IDE Visual Studio plugin for CxSAST adding a whole new look and feel to the plugin. Clicking ( ) takes you to the AppSec Coach. This version includes a free edition of AppSec Coach™ that covers 3 lessons (SQL Injection (SQLi), Cross-site scripting (XSS), XML Injection (XXE) and 6 coding languages (Java, .Net, PHP, Node.JS, Ruby, Python). The full and paid version will include 100+ lessons and additional coding languages.
	Custom description is now supported for the IDE Visual Studio plugin for CxSAST. Cx, CWE and now the custom description are available. Custom descriptions are generally created in CxSAST and provided for each query with an explanation of the associated risk. You can now view the unique customized description that best suits your own organizations procedures and best practices.
IDE – Eclipse	A new login option (SAML) has been added to the IDE Eclipse plugin for CxSAST and is available from the Authentication screen (Window > Preferences > CxViewer Preferences > Authentication). By checking the SAML option the authorized user performing the login will be navigated to the relevant SAML identity provider login page. The SAML login option is only available when the SAML feature is enabled in the CxSAST SAML Configuration screen.
IDE – IntelliJ	A new login option (SAML) has been added to the IDE IntelliJ plugin for CxSAST and is available from the CxViewer Preferences screen (File > Settings > Other Settings > CxViewer Preferences). By checking the SAML option the authorized user will be navigated to the relevant SAML identity provider login page. The SAML login option is only available when the SAML feature is enabled in the CxSAST SAML Configuration screen.
	The IDE IntelliJ plugin for CxSAST now supports Windows 10 with Java 8.
Plugins - Jenkins	CxSAST Jenkins plugin now supports Jenkins Pipeline – Jenkins Pipeline adds a powerful set of automation tools onto Jenkins, supporting use cases that span from simple continuous integration to comprehensive continuous delivery pipelines.
	The latest version of the CxSAST Jenkins Plugin now supports full report generation, via the Jenkins Dashboard.

Category	Features
Plugins – Bamboo	You can now integrate CxSAST with any Bamboo code build plan, enabling a Bamboo job/project to automatically initiate a CxSAST scan. Integration is achieved with our new CxSAST Bamboo plugin. Once downloaded from the central repository, the plugin is simple to install and configure.
API Integration - Project Branching	Project Branching API (CxAPI) allowing to automate process of project branching within the Checkmarx environment.
API Integration - CxOSA	The CxREST API for CxOSA provides developers with the ability to create client scripts for working with CxOSA projects, open source code scans and result reports. The REST API for CxOSA is open to all users with the appropriate authentication rights. Checkmarx's latest RESTful API's are documented using Swagger and is currently specified for open beta testing.

Engine

Category	Features
Supported Languages	Added new language support for Scala, thereby enabling to get results when scanning a project with Scala compatible files. The newly added language has been officially released for general availability.
	JavaScript ECMAScript 2015 (ES6) is supported as an open beta for testing
Supported Frameworks	ReactJS is now supported in this version. For more information about this support see the Known Limitations section (below)
	PHP framework scanning capability enhancements for bWAPP, Smarty, Symfony, CakePHP and Kohana.
	SAPUI5 is supported in this version.
	AKKA framework (for Scala) is now supported.
Incremental Scan Configuration	The following incremental scan main configuration keys are now available for this version: INCREMENTAL_SCAN_THRESHOLD (int) • Defines the maximum percentage of files changed to allow the incremental scan. • Valid values: 1-19 • Default value: 7 INCREMENTAL_SCAN_THRESHOLD_ACTION (string)

Category	Features
	• Defines the action to be taken when the threshold exceed in incremental scan. • FAIL – fail the scan. • FULL – switch to full scan. • Valid values: FAIL or FULL • Default value: FAIL

Resolved Issues

Category	Resolved Issues
Scan Improvements	Major advances in the engine providing significant reduction in false positives and false negatives across all supported languages.
Engine	Major improvements and fixes for the following languages: • Apex • Java • PL/SQL • JavaScript • PHP • ObjectiveC • C# • CCP • Ruby • VbNet

Known Limitations

Category	Known Limitations
Integration – CxOSA	CxOSA analysis results are not available in v8.4.2 for pre v8.4.2 scans. A new CxOSA scan is required in order to receive the full analysis results.
	In CxSAST, private scans are by default not displayed in the Projects State screen. This means that if a user creates either a new public project (which contains at least one private scan) or creates a new private project, an OSA analysis cannot be performed from the Project State screen for these private projects/scans.

Category	Known Limitations
AppSec Coach - External Services	In the new External Service setting page there is currently a limitation due to the fact that the automation process for AppSec Coach is still not activated automatically. This means that when clicking on the 'Activate' button you will get an error, unless the manual activation process was performed by Checkmarx support.
Languages - ReactJS	CxSAST can only scan ReactJS generated code (Using Babel) if it was generated according to the ECMAScript 5 standard.
	CxSAST is unable to scan generated code that is generated from ECMAScript 6 to ECMAScript 5.
	CxSAST is unable to Scan JSX syntax of React JS.
Languages - Scala	By design CxSAST doesn't support Scala scripting.

Supported Environments

Operating System

Windows (64-bit)	7, 8, 8.1, 10	**Windows Server**	2008R2, 2012, 2012R2

SQL Server

SQL	2008, 2008R2, 2012, 2012R2, 2014

Browsers

Microsoft Internet Explorer	10, 11, Edge
Apple Safari	6 and up
Google Chrome	43 and up
Mozilla Firefox	38 and up

IDE Plugins

Eclipse	3.6 - 4.5.1 (Mars), 4.6 (Neon)
IntelliJ	11 - 16
Visual Studio	2010, 2012, 2013, 2015

Build Servers

Jenkins	1.538 - 2.41
TFS	2013, 2015

Integration

Bamboo	5.9 to 5.15
SonarQube	4.5.4 - 6.1 (6.2 not supported)
Jira	5.0 - 7.0
Apache Maven	3.0 – 3.25, 3.3.9

Java Version

Java	6 (supported for Eclipse and IntelliJ IDE plugins only), 7, 8

Webserver

IIS	7.5 - 8.5

Supported Code Languages and Frameworks

CxSAST

Open Source Analysis (CxOSA)