Checkmarx CxSAST

Release Notes for 8.4.1

January, 2017

Contents

New Features and Changes

Application

Category	Features
SAML Integration	CxSAST has just become SAML 2.0 aware and can now be configured to act as a SAML Service Provider. SAML supports the user lifecycle by retrieving users from the Identity Provider (IdP) and defining them in CxSAST. This allows for more centralized and enhanced user management.
	A new sub-menu option (SAML) has been added to the Connection Settings menu in CxSAST (**Management** > **Connection Settings** > **SAML**). Selecting this option displays the SAML Configuration screen.
	A new SAML Configuration screen has been added to CxSAST (**Management** > **Connection Settings** > **SAML** > **SAML Configuration**). This new screen allows the authorized user to configure the SAML integration for authentication and user management.
	A new login option (SAML) has been added to CxSAST and is available from the existing CxSAST Login screen. By clicking on the SAML Login button the authorized user is navigated to the relevant SAML identity provider login page. The SAML login option is only available when the SAML feature is enabled in the SAML Configuration screen.
Query Viewer - Custom Description	A new option (Custom Description) has been added to the Query Viewer in the CxSAST application (**Management** > **Scan Settings** > **Query Viewer** > **Queries**). Descriptions are generally provided for each query with an explanation of the associated risk. You can now create a unique custom description to best suit your own organizations procedures and best practices.
Management - AppSec Coach	A new design has been added to the AppSec Coach™ in CxSAST adding a whole new look and feel. 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.
CxOSA - Local Source	A new option field (Local Source) has been added to the OSA tab **(Projects & Scans** > **Projects** > **OSA**) for Open Source configuration in CxSAST. This provides the authorized user with the capability to navigate and define a locally stored file or set of files for analysis when the user clicks on 'Run OSA'.

Category	Features
Utilities - CxOSA	A new utility (CxWhiteSourceRegistration) has been added to the CxSAST utilities library. This utility provides the ability to register directly to WhiteSource through CxOSA.

Integration & Plugins

Category	Features
Integration – MS-VSTS	Microsoft Visual Studio Team Services (MS-VSTS) is an extension of the Microsoft Visual Studio architecture that allows it to encompass development teams, with special roles and tools for software architects, developer specialties and testers. The new Checkmarx Plug-in for Microsoft Visual Studio Team Services is integrated seamlessly into the Microsoft's Software Development Life Cycle (SDLC), enabling the early detection and mitigation of crucial security flaws.
Integration – CxOSA-WS	A new CxOSA-WhiteSource integration option has been added to CxSAST application offering full support for a unified CxOSA-WhiteSource dashboard. This enables the authorized user with the capability to work with CxOSA projects in CxSAST as well as from within WhiteSource.
Integration – Maven	You can now integrate CxSAST with any Maven code build process, enabling a Maven project to automatically initiate a CxSAST scan. Integration is achieved with the new CxSAST Maven plugin. The plugin is simple to install and configure and once defined in the configuration the plugin is automatically downloaded from the central plugin repository.
Integration – Jenkins	You can now view the CxOSA vulnerabilities summary and libraries scan results in the OSA log file.
Integration – Jenkins	In order to support correct timeout for incremental scans the threshold unit for the Scan timeout (hours) parameter in the Jenkins System Configuration screen (**Jenkins Dashboard** > **Manage Jenkins** > **Configure System**) has been changed from hours to seconds.
Integration – IntelliJ	A new design has been added to the AppSec Coach™ in IntelliJ adding a whole new look and feel. 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.

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 is specified for open beta testing.
Incremental Scan	Since the officail release of the incremental scan feature, the speed and accuracy has been improved considerably.
Vulnerability Descriptions	New and updated vulnerability descriptions - giving more detailed guidance for code remediation.

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	Improvements and fixes for the following languages: Apex Java PL/SQL JavaScript PHP ObjectiveC C# CCP Ruby VbNet

Known Limitations

Category	Known Limitations
IDE – Visual Studio Plugin	Custom description is currently not supported in the IDE Visual Studio plugin even though Cx and CWE description are available.

Category	Known Limitations
Engine - Incremental Scan	At this time the incremental scan algorithm does not support receiving or renaming of files. In case a file was removed Checkmarx will not identify the change In case a file was renamed Checkmarx will identify it as new file
Engine - Incremental Scan	Due to limitations in the incremental scan algorithm (for example moving only three steps from the change) in less than 10% of the cases you may encounter differences between the full and incremental scan.