CHECKMARX
choose what developers use

Checkmarx CxSAST

Release Notes for 8.5.0 (GA Release)

October, 2017

Contents

New Features and Changes

Application

Category	Features
Setup	The new Checkmarx theme has been implemented into the latest version of the CxSAST installation and setup wizard. This has been redefined in order to match current Checkmarx branding.
	All Checkmarx icons (desktop and the Start menu) have been updated with the new Checkmarx logo in order to match the currently defined Checkmarx brand.
Supported Environments	Support for SQL Server 2016
Profile - Account Information	The CxSAST User Interface now supports French and Russian languages. The language selection option is available on the Account Information panel of the My Profile screen (My Profile > Account Information) and can be initiated by simply clicking on the Language drop-down and selecting the desired language.
Management - Application Settings	The 'All' languages option has been removed from a number of areas in CxSAST in order to provide accurate license validation enforcement (i.e. not to scan Java when the license doesn't support Java). This includes the Supported Languages panel (Management > Application Settings > License Details > Supported Languages) and also includes scan requests in REST APIs
	GOLang is now displayed on the Supported Languages panel of the License Details screen (Management > Application Settings > License Details > Supported Languages) in CxSAST. All languages are supported in CxSAST according to your Checkmarx license.
Management - Scan Settings	Four new predefined presets have been added to the presets list in the Preset Manager (Management > Scan Settings > Preset Manager): • NIST – defined according to National Institute of Standards and Technology compliance • FISMA – defined according to Federal Information Security Modernization Act compliance • STIG – defined according to Security Technical Implementation Guide compliance • XSS and SQLi only – defined for recommended best practice when starting to scan a new project in order to focus on the most important vulnerabilities first.

Category	Features
Management - CxOSA	A new panel (OSA Settings) has been added to the General Settings window (Management > Application Settings > General). The OSA Settings panel provides the following fields: • Organization Token – Displays the organization token provided by WS (read-only) • OSA Scan Options: • Match by File Name – Check to enable. If the SHA-1 Hash does not identify an open source library, a match is attempted using the provided filename. • Unrecognized Libraries – Check to enable. Libraries not identified by WS will appear in a separate section in the report. NOTE: Enabling either of these options will handover open source Filename to WS.
Management - Connection Settings	A new Sign SAML IdP Requests option has been added to the SAML Configuration screen (Management > Connection Settings > SAML). This option, once enabled, assures that every request sent to the Identity Provider is signed with a Service Provider certificate. NOTE: The SAML Version field has been removed from the SAML Configuration screen.
Open Viewer - Scan Results	Two new compliance options (FISMA 2014 and NIST SP 800-53) have been added to the Scan Results Severity filter in the Open Code Viewer for CxSAST (Dashboard > Project State > Open Viewer > Scan Results Severity).
Open Viewer - Scan Results	A new column (Number of Nodes) has been added to the Results panel in the CxSAST Code Viewer. This column provides the number of nodes in the attack vector provided by each result. Sorting, filtering and grouping options are available. This column is disabled by default and can be made available from the Columns selection tool.
Scan Results	The version of the PCI DSS compliance has been updated, from v3.1 to v3.2, in all areas of the CxSAST application including the code viewer, presets, reports, etc.
Report Generator	Two new categories (FISMA 2014 and NIST SP 800-53) have been added to the Report Generator (Dashboard > Project State > Create Report > Categories).

Audit

Category	Features
Setup	The new Checkmarx theme has been implemented into the latest version of the CxSAST installation and setup wizard. This change also reflects on the CxAudit installation and has been redefined in order to match current Checkmarx branding.
Audit View	CxAudit now enables exporting queries. When exporting queries, CxAudit also provides the capability to select only those queries that have been modified instead of having to look for each query manually.

Integration & Plugins

Category	Features
Visual Studio IDE - Support	Added support for Visual Studio 2017
Bamboo Plugin - Support	The CxSAST Bamboo plugin has completed its testing phase and now supports Bamboo version 6.0
Bamboo Plugin - Scan Task	A new setting parameter (Schedule interval based full scans) has been added to the Configuring a Scan Task screen in Bamboo. Check enables the scheduling of interval based full scans, when running incremental scans. This new parameter allows you to define a time range (interval begin and end) in which all scans will be full scans. For example, this could be used to ensure that daily runs would be incremental scans and nightly builds will be full scans, without having separate jobs. NOTE: This parameter is only available if the Enable incremental Scan option is enabled.
Jenkins Plugin	Improved Jenkins user interface has been updated in accordance with all Checkmarx plugins.
Jenkins Plugin (Pipeline)	New improved script generation option for Jenkins pipeline integration.
TeamCity Plugin	You can now integrate CxSAST with any TeamCity code build step, enabling a TeamCity job/project to automatically initiate a CxSAST scan. Integration is achieved with our new CxSAST TeamCity plugin. Once downloaded from the central repository, the plugin is simple to install and configure.
SonarQube Plugin	You can now integrate CxSAST with SonarQube enabling the display of current and trending security vulnerability information for a code project. Integration is achieved with our new CxSAST SonarQube plugin. Once downloaded from the central repository, the plugin is simple to install and configure. SonarQube is now available as beta for all customers.
CLI Plugin - CxOSA	New functionality (CxOSA) has been added to the CxSAST CLI plugin: • CxSAST & CxOSA Scan - run a CxSAST scan and CxOSA • CxOSA Scan - run CxOSA for an existing CxSAST project

Category	Features
Engine Auto Scaling API	New functionality (Engine Auto Scaling API) has been added to latest Checkmarx REST API library: • Get All Scan in Queue – gets details of all scan in queue • Get All Engine Details – gets details of all engine servers • Register Engine – register a new engine server • Unregister Engine – unregister an engine server • Get Engine Details – get details of a specific engine server • Update Engine – update an engine server This allows you to dynamically provision and remove scan engines according to your ever changing scan capacity demands. Swagger examples can be found at - Swagger Examples

Engine

Category	Features
Supported Languages and Frameworks	GOLang Beta Support: • GOLang is now available as beta for all customers • Frameworks/libraries supported: protobuf (by scanning Go generated code), Apache Cassandra
	Enhancements for Java: • Spring Dependency Injection - added support for scanning beans defined in XML files • Enhanced detection of dead code
	Enhancements for JavaScript: • Full support for ECMAScript 6 • Node.js enhancements for scanning CommonJS require and exports mechanism • Support for scanning Typescript transpiled into ECMAScript 6
	C# Support for New Structures: • Named and default parameters • Expression bodied functions • Static using

Category	Features
	• Name of operator • Index initializers
	Improvements for ASP.NET MVC • Improved framework parsing • Enhanced vulnerability coverage via improved queries
	Improvements for ASP.NET Razor • Improved parsing of Razor files • Added support for HTML Inputs and Outputs • Improvements detecting XSS and SQL Injections vulnerabilities
	ASP.NET CORE Beta Support • ASP.NET CORE is now available as Beta for all customers (activated by default)
	Improvements for Scala & Groovy • Support for Scala & Groovy languages has been improved to better identify objects in the source code. As a result, in the first scan after upgrading to 8.5, some of the results may be shown as 'Fixed' while others that replace them will appear as 'New'
General	Mobile support improvements (Android and iOS): • New queries • Added support for scanning Plist files in iOS (Configuration file) • Added support for scanning Gradle files in Android (Configuration file – replacement for manifest)
	Support for scanning lambda expressions across languages (C#, Scala, Java)
	Enhanced support to Polymorphism functionality
	Vulnerability coverage enhancements for multiple languages
	Engine licensing is now performed automatically by the Manager Server (Engine Servers no longer require their own license files). CxAudit still requires a local license file

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: • Java • JavaScript • C#

Known Limitations

Category	Known Limitations
LDAP Synchronization	If a user is created through LDAP synchronization, then the LDAP synchronization is disabled and then that user is manually moved to a higher role (company manager or higher) – the user may not get the new role's privileges.
CxOSA - Undetected Libraries & Match by Filename	Undetected libraries will report files in binary format (such as .dll & .jar), other files will not be reported. The reason for this is that WS saves undetected files in binary format only. Saving all file formats will infect the WS database.
Bamboo Plugin – Fonts display	Installing the Bamboo plugin (8.42.0) will affect the fonts displayed in all Bamboo build reports on Mac OS machines.

Supported Environments

Operating System

Windows (64-bit)	7, 8, 8.1, 10	**Windows Server**	2008R2, 2012, 2012R2, 2016

SQL Server

SQL	2008, 2008R2, 2012, 2012R2, 2014 * DBaaS not supported natively; AWS RDS can be used with some setup ** SQL Express not supported in production due to throughput and 10GB DB size limits imposed by Microsoft.

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, 2017

Build Servers

Jenkins	1.538 - 2.64

Jenkins (Pipelines)	2.x or later (1.6 - 2.0 not supported)
TFS	2013, 2015
Bamboo	5.9 to 6.10
TeamCity	2017.1.1 and up

Integration

Jira	5.0 - 7.0
SonarQube (Widget)	4.5.4 - 6.1
SobarQube (Plugin)	6.3 - 6.5
Apache Maven	3.0 – 3.25, 3.3.9

Java Version

Java	7 - 8

Frameworks

Microsoft .NET Framework	4.5.1 or above

Webserver

IIS	7.5 - 10

Supported Code Languages and Frameworks

CxSAST & Open Source Analysis (CxOSA)