Checkmarx CxSAST

Release Notes for 8.6.0 (GA Release)

February, 2018

Contents

New Features and Changes

Important Announcement - We are currently looking into a potential SAML Authentication issue in this release. If you use SAML, please refrain from installing this version until further notice.

Application

Category	Features
Setup and Configuration	A new Checkmarx License Agreement (EULA) screen has been implemented into the latest version of the CxSAST installation and setup wizard in order to all allow the user to accept/not accept the terms of the Checkmarx License Agreement. For silent installation, via the CxSAST CLI, the option to install CxSAST without the need to accept the license terms is still available.
Setup and Configuration	Long Path Support has been added to CxSAST. Traditionally, older versions of the Windows operating systems didn't support path or filenames with more than 260 characters, then with the release of Windows 10 and Windows Server 2016 provision for this issue was introduced. The following should be performed in order for the Long Path Support to be enabled and fully supported in CxSAST: • Enable Long Path Support in Windows 10 and Server 2016 • Enable Long Path Support in the CxSAST Application • Enable Long Path Support in CxAudit • Enable Long Path Support in CxSAST Server Settings • Enable Long Path Support in Git In order to use the Long Path Support feature, all Checkmarx components (CxEngines, CxPortal and CxAudit) must be Long Path Support enabled.

Category	Features
Integration - GIT	The Git/Github authentication methodology has been improved in this new version of CxSAST. The user is now able to use one of the following authentication methods for configuration with GIT: • No authentication at all (public repository) • Credential-based authentication • Token-based authentication • SSH-based authentication
Profile - Account Information	The default administration email defined during installation/upgrade has been changed from admin@cx to admin@cx.com. This email is displayed on the Account Information panel in the My Profile screen (My Profile > Account Information) and now conforms to our Codebashing email standards.
Management - Application Settings	The Engine Server panel has been removed from the Installation Information screen (Management > Application Settings > Installation Information). This panel has been replaced with the new Engine Management feature (see Engine Management).
Management - Application Settings	A new feature (Engine Sever Management) has been added to CxSAST. TheEngine Server Management feature is installed as part of the CxSAST installation and enables the following functionality: Interface for viewing real-time engine server status information: • Number of engine servers in the system (active and offline) • Status of each engine server (scanning, idle, blocked, etc.) • Location (URL) and scan size of each engine server Direct action options (single) include: • Register engine server • Edit engine server • Unregister engine server • Block/unblock engine server The Engine Server panel has been removed from the Installation Information screen (Management > Application Settings > Installation Information) to accommodate this new feature.

Category	Features
Management - Connection Settings	The CxSAST user now has the capability to save the LDAP settings in the LDAP Sever Settings screen (Management > Connection Settings > LDAP Servers) without having to perform and validate the connection test first. Validating the connection can now be performed at a later stage. The Test Connection button has also been moved from its previous location, at the top of the LDAP Servers screen to the bottom of the LDAP Server Settings panel.
Management - Scan Settings	A new preset (OWASP Top 10 2017) have been added to the predefined presets list in the Preset Manager (Management > Scan Settings > Preset Manager). This new preset further enhances the already extensive Checkmarx preset library with regards to OWASP compliance.
Management - Application Settings	The External Services screen (Management > Application Settings > External Services Settings) has been updated in coordination with the implementation of Codebashing into CxSAST. This was added at the end of 8.5.0. The enable non-anonymous data collection (email hashing) option has also been removed from the UI as well as the enablement procedure.
Open Viewer - Scan Results	A new results filtering option (OWASP Top 10 2017) has been added to the Scan Results Severity filter in the Open Code Viewer for CxSAST (Dashboard > Project State > Open Viewer > Scan Results Severity).
Report Generator	A new category (OWASP Top 10 2017) has been added to the Report Generator (Dashboard > Project State > Create Report > Categories).

Audit

Category	Features
Setup and Configuration	A new Checkmarx License Agreement (EULA) screen has been implemented into the latest version of the CxAudit installation and setup wizard in order to all allow the user to accept/not accept the terms of the Checkmarx License Agreement.
Audit Client	The folders in the Workspace View in CxAudit are now presented in an hierarchical tree structure (like in windows explorer). This makes it easier to navigate and find scanned project files. Configuration Key is CXAUDIT_TREE_VIEW_FLAT and default is set to false (new hierarchical tree structure). True sets the regular TreeView structure.

Integration & Plugins

Category	Features
IDE Support - Logs	All Checkmarx IDE plugins now add their own version into the log\console using the following syntax: $<plugin name> Plugin Version: $<version>.
Jenkins - Plugin Support	The Checkmarx Jenkins plugin now supports Jenkins 2.91
Jenkins - Plugin Global and Scan Configuration	A new drop-down selection method (Credentials) has been added to the CxSAST Global Configuration and Scan Settings screen in the CxSAST Jenkins plugin. This method is now mandatory for users that already have Jenkins credentials, as defined in Jenkins, and would like to use the same credentials with the CxSAST Jenkins plugin. The old method may still work for existing jobs.

Category	Features
Jenkins - Plugin Scan Configuration	A new drop-down selection option (Fail the build for new issues of the following severity or higher) has been added to the CxSAST Scan Configuration screen in the CxSAST Jenkins plugin. This new option enables the user to fail the build according to the defined severity (or higher). This options works in addition to the regular thresholds (e.g. if "x" total high issues were found OR at least 1 new issue, fail the build). This option is only available if the "Enable vulnerability threshold" parameter is enabled.
Jenkins - Plugin Scan Results	The scan results in the Checkmarx Jenkins plugin (CxSAST Summary) have been updated to include new and recurrent scan issues. The status of a vulnerability is recurrent if it was already discovered in a previous scan. The status of a vulnerability is new if it was discovered for the first time, or if it was re-opened after being resolved in a previous scan.
Jenkins - Plugin Scan Results	The scan results in Checkmarx Jenkins plugin have been updated in accordance with running a scan in asynchronous mode. A full report has now been added to the Jenkins job for asynchronous scans. The following note has been added for cases where the full report may not be displayed; "Job is configured to run the Checkmarx scan asynchronously. This specific build's scan result cannot be displayed in this mode. Any results displayed are from the previous successful scan"
Jenkins - Plugin Scan Results	The Checkmarx Last Scan Results link and the related scan report have been removed from the CxSAST Jenkins plugin main dashboard. All related scan results are now provided from the CxSAST Summary.
Jenkins - Plugin CxOSA Scan	The Checkmarx Jenkins plugin now creates CxOSA scan by sending SHA1 instead of binaries.
Bamboo - Plugin Global Configuration	A new setting parameter (Deny new Checkmarx project creation) has been added to the Global Configuration screen in Bamboo. Enabling this option will prohibit the creation of new projects in Checkmarx, or assigning an existing project to a different team. Disabling this option allows these actions.

Category	Features
Bamboo - Plugin CxOSA Scan	The Checkmarx Bamboo plugin now creates CxOSA scan by sending SHA1 instead of binaries
TeamCity - Plugin Scan Results	The Failure result in the TeamCity results summary has been expanded in order to display more information about the actual failure.
TeamCity - Plugin Scan Results	Build failure is now written to the log.
TeamCity - Plugin CxOSA Scan	The Checkmarx TeamCity plugin now creates CxOSA scan by sending SHA1 instead of binaries
SonarQube - Plugin Support	The Checkmarx SonarQube plugin now supports SonarQube 6.7 (LTS)
SonarQube - Plugin Apex Support	The Checkmarx SonarQube plugin now supports the Apex coding language.
SonarQube - Plugin Presets	The Checkmarx SonarQube plugin now supports the automatc creation of Checkmarx quality profiles (CxSAST presets). The user that installs the a language plugin for SonarQube will now have an automatically created quality profiles for CxSAST code scanning. Each quality profile created contains all relevant rules for that language.
SonarQube - Plugin Apex Support	The Checkmarx SonarQube plugin now supports the Apex coding language.
SonarQube - Plugin Presets	The Checkmarx SonarQube plugin now supports the automatc creation of Checkmarx quality profiles (CxSAST presets). The user that installs the a language plugin for SonarQube will now have an automatically created quality profiles for CxSAST code scanning. Each quality profile created contains all relevant rules for that language.
SonarQube - Plugin Scan Results	The Checkmarx SonarQube plugin report UI has been updated to correspond with the design and layout of other CxSAST plugins.

Category	Features
SonarQube Plugin - Rules and Presets	Rules & Presets for the SonarQube plugin have been upgraded according to the latest CxSAST engine.
MS-VSTS Plugin - CxOSA Scan	The Checkmarx MS-VSTS plugin has been upgraded in order to support the following: • CxOSA scan • CxSAST and CxOSA Reports
MS-VSTS Plugin - CxOSA Scan	The Checkmarx MS-VSTS plugin now creates CxOSA scan by sending SHA1 instead of binaries.
MS-VSTS - Plugin Presets	The Checkmarx MS-VSTS plugin has been upgraded in order to support 'Custom Presets'. Custom presets are provided in cases where the desired preset is not available from the Checkmarx presets list. Note that specifying a Custom Preset will override any predefined presets.
MS-VSTS Plugin Supported Environments	The Checkmarx MS-VSTS Plugin now supports both TFS 2015 and VSTS
WhiteSource Integration	A new version of the CxOSA-WS utility has been added to WhiteSource integration allowing you to easily register to WhiteSource through CxOSA. You can download the latest version of the CxOSA-WS utility from Checkmarx Utilities.

CLI / API

Category	Features
CxCLI Plugin - Authentication	A token-based authentication and login method has been introduced into the latest version of the CxSAST/CxOSA CLI plugin (v8.60.0 and up).

Category	Features
CxCLI Plugin - Configuration	The CxSAST scan is, by default, run in synchronous mode (Scan). This means that the CLI initiates the scan task and the scan results can be viewed in the CLI and in the log file created. Asynchronous mode was introduced into the last version of the CxSAST/CxOSA CLI plugin. In asynchronous mode (AsyncScan), the scan task ends when the scan request reaches the scan queue, as a result the scan results can only be viewed via the CxSAST web application. This was added at the end of v8.50.0
CxCLI Plugin - Configuration	CLI Exit/Error code were introduced into the last version of the CxSAST/CxOSA CLI plugin. These codes help in identifying and troubleshooting issues. This was added at the end of v8.50.0
CxCLI Plugin - Configuration	CxCLI Plugin – Configuration • -OsaArchiveToExtract <files list> - Comma separated list of file extensions to extract in the OSA scan. For example: -OsaArchiveToExtract *.zip extracts only files with .zip extension (Optional). • -OsaScanDepth <OSA analysis unzip depth> - Extraction depth of files to include in the OSA scan (Optional)
CxARM-API - CxSAST	A new Risk Management API is now available. The API is based on OData and provides the ability to query the SAST and OSA findings, allowing you to analyze the security status of the projects in the organization. OData allows you to aggregate, filter, count and group all the available data.
CxREST API - Versioning	Versioning has been introduced into to the latest version of the CxREST API. CxSAST is installed with the latest version of the CxREST API (i.e. v=1.0). In order to use other versions of the CxREST API you will need to specify the desired version for each API call. Note that not specifying the version will automatically apply the latest version and may cause your script/code to break.
CxREST API - Authentication	Token-based authentication / login (OAuth 2.0) functionality has been added to the latest version of the CxREST API.

Category	Features
CxREST API - General	New functionality for the General API set has been added to latest CxREST API library: • Get All Project Details - GET /projects • Create Project with Default Configuration - POST /projects • Get All Teams - GET /auth/teams • Get Project Details by Id - GET /projects/{projectId} • Get Report(s) by Id - GET /reports/sastScan/{reportId} • Get Report Status by Id - GET /reports/sastScan/{reportId}/status • Register Scan Report - POST /reports/sastScan • Upload Source Code Zip File - POST /projects/{projectId}/sourceCode/attachments • Set Remote Source Setting to GIT - POST /projects/{projectId}/sourceCode/remoteSettings/git • Set Remote Source Setting to TFS - POST /projects/{projectId}/remoteSettings/tfs • Set Remote Source Setting to Shared - POST /projects/{projectId}/remoteSettings/shared • Set Remote Source Setting to Perforce - POST /projects/{projectId}/remoteSettings/perforce • Set Remote Source Setting to GIT using SSH - POST /projects/{projectId}/remoteSettings/git/ssh • Set Remote Source Setting to SVN using SSH - POST /projects/{projectId}/remoteSettings/svn/ssh
CxREST API - CxOSA	New functionality for the Engine Auto Scaling API set has been added to latest CxREST API library: • Get Engine Details - GET /sast/engineServers/{id} (v8.6.0 and up) • Get All Scan Details in Queue (8.6.0 and up)
CxREST API - CxSAST	New functionality for the CxSAST API set has been added to latest CxREST API library: • Get All Preset Details - GET /sast/presets • Get SAST Scan Details - GET /sast/scans/{id} • Get Preset Details - GET /sast/presets/{presetId}

Category	Features
	• Get All Engine Configurations - GET /sast/engineConfiguration • Get Scan Settings - GET /sast/scanSettings/{projectId} • Get Engine Configuration - GET /sast/engineConfigurations/{id} • Create New Scan – POST /sast/scans • Define SAST Scan Settings - POST /sast/scanSettings

Engine

Category	Resolved Issues
Application Security	New queries for Mobile security (Android and iOS)
	More than 100 query bug fixes related to AppSec research
	New preset for OWASP top 10 2017
Languages/Frameworks	Typescript Native support
	Angular 4 support on top of Typescript Compatible with Angular 2.X +
	.NET Core 1.1
	Google Guice support - dependency injection framework for Java
General	Ability to resolve Pointers and Aliasing for Object Oriented Languages
	The engine log now contains extended details regarding languages detected in the scan

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.

Known Limitations

Category	Known Limitations
Setup and Configuration	The SQL Express 2008 installation included in CxSAST is not supported by Windows 2016. In this case you will need to install a newer version of SQL Express separately before launching the CxSAST installation.
CxOSA - Plugin Support	Only OSA plugins (v8.5.0 and above) will be supported in the 8.6.0 version of CxSAST. OSA Plugins (8.4.2 and lower) will not be supported.
TFS 2015 Environment	Due to a Microsoft confirmed issue in TFS 2015, in case you do not use an http proxy, you must still fill-in our proxy field with a string. Suggested string would be the word noproxy.

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, 2016 * 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 – 2.91

Jenkins (Pipelines)	2.x or later (1.6 - 2.0 not supported)
TFS	2013, 2015
Bamboo	5.9 to 6.2
TeamCity	2017.1.1 and up

Integration

Jira	5.0 - 7.0
SonarQube (Widget)	4.5.4 - 6.1
SobarQube (Plugin)	6.3 - 6.7
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)