

8.9.0 Hotfix (1-24)

修正された問題と改善点

※ Hotfixは、別段の指示がない限り、CxManager、CxEngines、CxAuditをインストールしているマシンで適用する必要があります。分散環境においては、ポータルマシンへのインストールも必要です。

【注】 SQL 2008 と SQL 2008R2 は8.8.0 HF13以降ではサポートされていません。

カテゴリ	修正された問題と改善点
HF1	中国語の脆弱性クエリ説明ページを用意
	Java言語における、Apache Velocityのサポートを追加
	Java言語における、SQLインジェクションに対するクエリを改良
	スキャンが停止してしまう問題を修正
	CxOSAにおけるUIの微調整とログ機能の改良を実施

カテゴリ	修正された問題と改善点
HF2	CPP、Kotlin、GoおよびC#.Net言語に対するサポートを改善
	キューの管理機能を改良
	エンジンの開始と終了に要する時間を短縮
	インクリメンタルスキャンのロジックを改良
	高可用性 (high availability) 環境においてデータ分析画面を開いた際にエラーが発生する問題を修正
	800 MBを超えるファイルのXML出力が途中終了する問題を修正
	適切なLOC範囲が設定されたにもかかわらず、スキャンが開始されないことがある問題を修正
	ポリシー違反タブが表示されない問題を修正

レポート出力が失敗する問題を修正
コード変更無しにインクリメンタルスキャンを実施後に、「マネージメント/保守/データ保持」画面でスキャン結果の削除を選択すると、全スキャンログが削除されてしまう問題を修正
REST APIのブランチ作成機能を使った際に、プリセットなどの設定がブランチ先プロジェクトにコピーされない問題を修正
JavaScriptエンジンの構文解析において、ウォッチドッグタイマが適切に動作しない問題を修正
設定キー"UnzipLocalDrive"を有効にしたとき、スキャン後に削除されるはずのzipファイルが残ってしまう問題を修正
コード変更が無いときにインクリメンタルスキャンを実施すると、一時ファイルがExtSrcフォルダから削除されない問題を修正
同期処理中に、ActiveMQサービスの再起動が停止する問題を修正
GetFullTeamName機能が、間違った結果を返す問題を修正
複数チームが利用しているクエリを上書きした際に、上書きされたクエリがひとつのチームに対してしか表示されない問題を修正
ログの出力場所をデフォルトから変更した場合、ダウンロードしたログにアプリケーションログが含まれない問題を修正
ユーザー & チーム画面のアクセス制御情報をCSVファイルに出力できないことがある問題を修正
コード変更無しにインクリメンタルスキャンが実施された場合に、その動作がスキャンコメントに記録されない問題を修正
コード変更無しにスキャンが実施された場合に、正しいキュー時間がCxDBのTaskScansテーブルに保存されない問題を修正
CxAuditSrcディレクトリパス が259文字を超える場合、CxAuditがファイル名のコピーに失敗する問題を修正
インクリメンタルスキャンの結果に、最後に実施したフルスキャンのNOT_EXPLOITABLE結果を含むための機能を追加 この機能を有効にするためには、CxDBの CxComponent Configurationテーブル上の INCREMENTAL_SCAN_MERGE_NOT_EXPLOITABLE_RESULTSキーの値をtrueにしてください。
CxSASTポータルサイトの脆弱性を修正 (Telerikセキュリティパックを適用)

カテゴリ	修正された問題と改善点
HF3	HF3から、ひとつのインストーラで「GUIでの適用」と「コマンドラインでの適用」が可能になりました。適用方法の切り替えは、オプションで行います。コマンドラインでの実行には、cmdオプションを付与してください。
	最新バージョンのNPMのCxOSAスキャンが失敗する問題を修正
	大量のファイルのCxOSAスキャンが失敗する問題を修正
	CxOSAの結果表示画面で、オープンソースライブラリごとにパッケージマネージャー情報を表示するように改良
	オーケストレーション管理（ポリシー管理）機能のセキュリティに関連する問題を修正

カテゴリ	修正された問題と改善点
HF4	PHPとGo拡張子を持つファイルに対するCxOSAスキャンが失敗する問題を修正
	Kotlinプロジェクトに対するCxSASTスキャン失敗する問題を修正
	JavaScript構文解析に関連する問題を修正し、JavaScriptプロジェクトにおける脆弱性検出能力を強化

カテゴリ	修正された問題と改善点
HF5	CxSASTのセキュリティに関連する問題を修正
	ユーザーやチーム情報がCSVファイルに出力できない問題を修正
	コード変更無しにインクリメンタルスキャンが実施された場合に、TaskScansテーブルに不正確なスキャン情報が記録される問題を修正
	ローカルディスク上に一時ファイルが蓄積されてしまう問題を修正
	中国語版の脆弱性クエリの説明ページを更新
	PHP言語における、クラスのメンバーアクセスのデータフロー構築処理を改良
	Ruby言語における、クラス変数の宣言に対する解析処理を改良

	PHP言語において過剰検出が発生する問題を修正
	高可用性 (high availability) 環境でZIPファイルをアップロードした際、最悪の場合、CxOSAスキャンが失敗する問題を修正
	オーケストレーション管理 (ポリシー管理) オプションがインストールされていない場合に発生するCxOSA結果表示画面の不具合を修正

カテゴリ	修正された問題と改善点
HF6	ローカルドライブ上でZIPファイルをスキャンすると、ファイル解凍に失敗するCxOSAの問題を修正
	Tomcatを利用し、ポリシー管理機能のパフォーマンスを向上
	ポリシー管理機能のアップグレードと複雑な環境構築に関連する問題を修正
	エンジンのパフォーマンス向上 (メモリの解放) のためにデフォルトでは有効 (true) に設定されているガベージコレクション機能を無効化するスイッチを追加。大容量のメモリを搭載したシステム (マルチコアシステムなど) の利用時に、ガレージセールコレクションの実施がスキャン時間に影響を与える問題を解消。エンジン設定キー'MANUAL_CALL_GC_COLLECT'の値をfalseに設定することで無効化できます。
	しきい値を超えたことによりインクリメンタルスキャンが取り消され、フルスキャンが実行された場合に、新しいベースライン (以降に実行されるインクリメンタルスキャンの変更率算出の基準) として記録されるように改良。CxSAST上で、本ケースのスキャンが、フルスキャンとして表示されない問題も修正。

カテゴリ	修正された問題と改善点
HF7	データベースのタイムアウトが発生した場合に、同じスキャン結果が複数回保存される問題を修正
	新しいプロジェクトをCxOSAでスキャンした際に、ライブラリがパッケージマネージャーでデフォルトで識別されるように改良

カテゴリー	修正された問題と改善点
HF8	[Python] – "self"を使用した解析における、フローや定義の検出精度を改善
	[Python] – 関数定義内のパラメーターとその関数内での使用箇所間のフロー検出精度を改善
	日本語および中国語の脆弱性クエリ説明ページとサンプルコードを用意
	コードの変更が無い場合でも強制的にフルスキャンを実行するREST-APIのオプションを追加
	GITリポジトリに対するアクセストークンの扱いに関連するセキュリティを改善
	潜在的クロスサイトスクリプティングやCookie処理に関連する脆弱性を修正

カテゴリー	修正された問題と改善点
HF9	Pythonの解析精度を改良

カテゴリー	修正された問題と改善点
HF10	JavaScript解析時に内部オブジェクト（XPathProviderとCxList）間で不整合が発生する問題を修正
	Apex Visual Forceのコードを解析した際に、誤った箇所に対する指摘がされてしまう問題を修正
	Rubyのデータフローで発生していた問題を修正
	失敗したスキャンを終了できない問題を修正

カテゴリー	修正された問題と改善点
HF11	認証プラグインの同期に関連する問題を修正
	UIでのスキャン状態の更新プロセスのパフォーマンスを改善

	パフォーマンスに問題がある場合に、ベストフィックスロケーションの自動計算を無効にする機能を追加
	ベストフィックスロケーションを計算する機能のパフォーマンスを改良
	ベストフィックスロケーションの内部処理で発生する、データベースロックの問題を修正
	CxSAST REST API経由でGitリポジトリ定義を設定する機能を改良
	LDAPチームとCxSASTグループのプロパティ間で大文字小文字の差異があった場合にLDAPのユーザー同期に失敗する問題を修正
	ルートディレクトリ配下に配置したソースの解析時に、バックスラッシュが除外されてしまう問題を修正
	ポスト・スキャンアクション設定でメールアドレス変更が行われた場合、指定アドレスに重複メールが送信される問題を修正
	ポータル上とSOAP API間での、SimilarityID不一致の問題を修正
	Git SSL接続のURLにてハイフンをサポート
	ポータルのUIにて[スキャン開始アクション]、[スキャン成功後アクション]のボタンが隠れてしまう問題を修正
	クッキーのセキュリティ問題により、Swagger経由でのログインに失敗する問題を修正
	CxOSAレポートのインベントリライブラリ項目にバージョン番号を追記
	CxOSAライブラリページが更新されない問題を修正

カテゴリー	修正された問題と改善点
HF12	フロントエンドにおけるKotlinをサポート改良。Kotlinに対するサポートを有効にするには、CP95-Kotlinルールセットコンテンツパック（Cobolを含む）をインストールする必要があります。
	PL/SQLの予約語の解析ができない問題を修正
	Scalaの解析で発生していたいくつかの問題を修正

カテゴリ	修正された問題と改善点
HF13	プロジェクトごとに類似IDを計算する設定（‘RESULT_ATTRIBUTES_PER_SIMILARITY’の値をfalseに設定）にした場合に結果がレポートビューアに表示されない問題を修正
	XMLレポートを出力する際、ポータル（REST）上とSOAP APIの間での、SimilarityIDの計算結果が一致しない問題を修正
	データベースのパスワードに特殊文字が含まれる場合に、oData APIが使用できるように改良
	スキャンが失敗したにも関わらず、ポータル上で完了と表示される問題を修正

カテゴリ	修正された問題と改善点
HF14	CxOSAレポートのリスク項目において、事前で定義した値よりフィールドが長くなってしまふ問題を修正
	レポートビューアにおいて、Ver.8.9より前のスキャン結果の一部のクエリ名が表示されない問題を修正
	重大なセキュリティ上の問題を修正
	JIRAクラウドへの接続時の互換性に関連した問題を修正

カテゴリ	修正された問題と改善点
HF15	Linux環境向けのJSONマクロファイル内のグローバルインクルード処理を修正

カテゴリ	修正された問題と改善点
HF16	スキャン関連ファイルのクリア処理が失敗し、ストレージの逼迫が時折発生してしまう問題を修正
	結果ビューア内で選択された結果の先頭箇所から、クエリの説明ページに遷移できないことがある問題を修正
	TFS連携に問題がある場合、すべてのフォルダがスキャンされないことがある問題を修正
	複数のクエリが同時に更新されたときに、CxSAST OData APIから誤った結果が返されることがある問題を修正

カテゴリー	修正された問題と改善点
HF17	インストールパッケージ内のJava実行環境を、 OpenJDK 8u242 に変更
	ActiveMQ を最新版にアップグレード
	高負荷な状態になった際に、クエリタイムアウトによるスキヤンの失敗が起こらないようにM&Oを改善

カテゴリー	修正された問題と改善点
HF18	<p>CxEngineConfigurationKeysMetaテーブルの MAX_NUMBER_OF_RESULTS キーで、クエリごとの結果の最大保存件数が定義できるようになりました。</p> <ul style="list-style-type: none"> 制限無しで結果を保存する場合は、デフォルト値の-1を使用 最大数を定義する場合は、任意の値（例：クエリごとの結果保存件数を100までに抑えたい場合は"100"）を設定

カテゴリー	修正された問題と改善点
HF19	「プロジェクト」と「全スキャン」画面の UI を改良
	Gitリポジトリでタグを使用した場合、git clone ができずにスキャンが失敗する問題を修正

カテゴリー	修正された問題と改善点
HF20	（ユーザーによるコメント入力があった場合）ユーザーコメントも No Change コメントに含むように、 No Code Change スキャンの自動コメント挿入ロジックを改善
	取得した結果に対する内部プロセスが完了するまで、スキャン終了アイコンが表示されないように改善
	リポジトリのパスに -b を含むプロジェクトが新規作成された時に発生していた Gitリポジトリへの接続問題を修正
	スキャン結果のCSVファイル出力が失敗することがある問題を修正
	JIRA連携で、大きなJSONファイルの処理にも対応
	複雑な構造のプロジェクトをスキャンしたときに、CxOSAのライブラリ検出数が少なくなる問題を修正

カテゴリー	修正された問題と改善点
HF21	<p data-bbox="421 226 995 264">Apexの Reflected_XSS クエリを改良</p> <p data-bbox="421 297 1326 443">システムのメモリ容量低下によるエンジンの異常停止を回避するために、新しいスキャン停止メカニズムを導入。この機能の有効化・設定には CxEngineConfigurationKeysMetaテーブルの以下のキーを使用します。</p> <ul data-bbox="432 454 1326 949" style="list-style-type: none"> • WATCHDOG_ABORT_SCAN_ON_LOW_MEMORY (デフォルト値：false - 無効) • WATCHDOG_ABORT_SCAN_ON_LOW_MEMORY_MAX_USAGE_PERCENT (デフォルト値：96%) スキャン停止の基準となるシステム全体のメモリ使用割合の上限値を設定 • WATCHDOG_ABORT_SCAN_ON_LOW_MEMORY_MIN_AVAIL_MB (デフォルト値：1024Mb) MAX_USAGE_PERCENTのチェック実施の基準となる、空きメモリ量の下限値を設定 • WATCHDOG_ABORT_SCAN_ON_LOW_MEMORY_COUNTER (デフォルト値：5回) スキャン停止を実施する基準となるメモリ不足連続発生回数を設定 <p data-bbox="432 987 1326 1133">システムのメモリ容量低下時にファイルのパーズ処理を停止するための新しいメカニズムを導入。この機能の有効化・設定には CxEngineConfigurationKeysMeta テーブルの以下のキーを使用します。</p> <ul data-bbox="432 1144 1139 1406" style="list-style-type: none"> • ABORT_FILE_PARSING_ON_LOW_MEMORY (デフォルト値：false - 無効) • MEMORY_WATCHDOG_MAX_USAGE_PERCENT (デフォルト値：95%) • MEMORY_WATCHDOG_MIN_AVAIL_MB (デフォルト値：2048Mb) • MEMORY_WATCHDOG_COUNTER (デフォルト値：5) <p data-bbox="421 1435 1326 1541">設定によってはスキャン結果の不整合を引き起こすことがあるため、事前に弊社サポート (ss_support@toyo.co.jp) にお問い合わせください。</p>

カテゴリー	修正された問題と改善点
HF22	<p data-bbox="421 1756 1337 1832">プライベートキーを使用した際の BitBucket の Git リポジトリとの連携機能を改善</p> <p data-bbox="421 1865 959 1904">BitBucket 接続用APIの不具合を修正</p> <p data-bbox="421 1937 1326 2049">プロジェクトスキャン結果のビューページのツールバーからフルスキャンやインクリメンタルスキャンが開始できないことがある問題を修正</p>

	無効な文字列が入力されると SAST タブエディターが応答しなくなる問題を修正
	JIRA連携において、Unicodeエンコードをサポート
	レポーターフィールドが必須となっている場合、JIRAクラウドへのスキャン結果の登録が失敗する問題を修正

カテゴリ	修正された問題と改善点
HF23	インストーラーを再構成・改良

カテゴリ	修正された問題と改善点
HF24	<p>スキャン対象から除外するファイルを"* *"を含むファイル名で指定した際、意図したファイルではなく、その指定条件に合致する名前を持つフォルダがスキャン対象から除外されてしまう問題を修正</p> <p>制限事項</p> <p>スキャン対象から除外するファイルやフォルダの名前をUI上で指定する際に、"* *"を使うことはできません。</p>