OpenText™ Core Application Security

リリース ノート

Version : 26.2

PDF Generated on : April 22, 2026

Table of Contents

1. リリース ノート

このドキュメントでは、OpenText™ Core Application Security (Fortify on Demand) リリース 26.2.0 に適用される新機能、インストールとアップグレードの注意事項、既知の問題、および回避策について説明します。
この情報は、製品ドキュメントの他の場所では入手できません。この製品のユーザー ガイドは、製品ドキュメントの Web サイトで入手できます。
OpenText Core Application Security (Fortify on Demand) - ドキュメント | Micro Focus

1.1. Fortify 製品名の変更

OpenText では、以下の製品名を変更中です。

以前の名前	新しい名前
Fortify Static Code Analyzer	OpenText™ Static Application Security Testing (OpenText SAST)
Fortify Software Security Center	OpenText™ Application Security
Fortify WebInspect	OpenText™ Dynamic Application Security Testing (OpenText DAST)
Fortify on Demand	OpenText™ Core Application Security
Debricked	OpenText™ Core Software Composition Analysis (OpenText Core SCA)
Fortify Applications and Tools	OpenText™ Application Security Tools
Fortify Aviator	OpenText™ Core SAST Aviator (SAST Aviator)

製品のスプラッシュ ページ、マストヘッド、ログイン ページ、および製品が表示されるその他の場所で製品名が変更されています。名前の変更は、製品の機能を明確にし、Fortify Software 製品を OpenText と合わせることを目的としています。ドキュメントのタイトル ページなど、場合によっては、古い名前が括弧で囲んで示されることもあります。今後の製品リリースでは、さらに多くの変更が行われる見込みです。

1.2. エンジンとルールパックの更新

OpenText Core Application Security 26.2.0 には、次のバージョンのエンジンとルールパックが含まれています。

- **Fortify Software Security Content 26.1.0:**
  OpenText Core Application Security の Fortify Software Security Content 26.1を実装します。詳細については、「Fortify Software Security Content 26.1」を参照してください。
- **OpenText Static Application Security Test 26.1.0:**
  OpenText Core Application Security の OpenText SAST (Fortify Static Code Analyzer) バージョン 26.1を実装します。

1.3. 新機能

AI を活用した SAST

Core Application Security は、次世代 SAST アーキテクチャによって実現された、12 種類のプログラミング言語をサポートする、AI を活用したスキャン機能を導入しました。この強化されたアーキテクチャにより、新しい言語の導入が大幅に加速され、将来の言語サポートをより迅速かつ効率的に提供できるようになります。この機能を有効にするため、[管理]→[設定]→[SAST] に、新しい設定項目 [AI を活用した SAST の有効化] が追加されています。

詳細については、『Core Application Security ユーザー ガイド』の「SASTの構成」を参照してください。

Note
この機能はリリース済みですが、現時点ではご利用いただけません。後日有効になります。

修復ダッシュボードの機能強化

Core Application Security 26.2では、新しい修復ダッシュボードに以下のグラフが追加されました。

- 重大度別のレビュー範囲 - 各重大度レベルでレビューされた、特定されたセキュリティ問題の割合を示します。
- 重大度別の修復範囲 - 重大度レベル別に、修復された問題の割合を示し、リスクの高い脆弱性がどれだけ効果的に対処されているかを強調表示します。
- 問題修復の傾向 - 重大度別の月ごとの修復傾向を表示して、計画策定、優先順位付け、およびリソース配分を支援します。
- 頻繁に再発している問題 - 最も頻繁に再発しているセキュリティ問題のカテゴリをランキング形式で表示し、より詳細な根本原因分析やプロセス改善が必要な領域の特定を支援します。
- スキャン タイプ別のレビュー範囲 - スキャン タイプに基づいて、修復された問題の割合を表示することで、さまざまなセキュリティ テスト手法における修復の有効性を示します。
- スキャン タイプ別の修復範囲 - スキャン タイプに基づいて、修復された問題の割合を表示します。

- SAST Aviator の採用 - 管理対象アプリケーション全体における SAST Aviator の採用状況を視覚的に表示します。
- 平均修復時間 - このビューは、修復期間が改善したことを前年との比較で強調表示し、前年比 (YoY) の変化を明確に示します。
- 重大度別の平均修復時間 - 重大度レベル別に分類された平均修復時間を表示し、リスクの高い問題がどれだけ効果的に優先付けされているかを示します。
- 問題再発率 - 再発している問題の現在の割合と正確な件数を表示します。
- SAST Aviator の投資利益率 (ROI) - SAST Aviator によって達成された、コスト節約と時間の効率化の推定値を示し、脆弱性検出と修復を早期に行うことのビジネス価値を強調表示します。

詳細については、『Core Application Security ユーザー ガイド』の「新しいダッシュボード」を参照してください。

2FAで保護されたDASTスキャン

Core Application Security は、二要素認証 (2FA) で保護されたアプリケーションの動的スキャンをサポートするようになりました。この機能強化により、強力なアクセス制御を維持しながら、多要素認証を必要とするアプリケーションの安全な評価が可能になります。この機能をサポートするため、DAST 設定フォームに構成フィールドが追加されました。これにより、チームは必要な認証情報を2FA応アプリケーションに指定し、動的スキャンを正常に実行できるようになりました。

詳細については、『Core Application Security ユーザー ガイド』の「動的スキャンの構成」を参照してください。

SCIM統合サポート

Core Application Security 26.2 では、SCIM 2.0 標準に準拠した新しい SCIM 統合機能が導入され、顧客の ID プロバイダ (IdP) とテナント間におけるユーザーとグループの自動プロビジョニングが可能になりました。この機能をサポートするため、テナントポータルの [管理] → [ユーザー管理] に [SCIM 統合] タブが追加されました。この専用インターフェイスにより、SCIM ベースのプロビジョニングの一元的な構成と管理が可能になります。

詳細については、『Core Application Security ユーザー ガイド』の「SCIM (System for Cross-domain Identity Management) の構成」を参照してください。

シングル サインオン (SSO) を使用した SCIM 統合

さらに、SCIM のプロビジョニングをシングルサインオン (SSO) 経由で直接有効化できるようになりました。SSO 構成から SCIM を有効にすることで、組織は単一かつ一元的なワークフロー内で、ID 認証とライフサイクル管理を効率化できます。

詳細については、『Core Application Security ユーザー ガイド』の「OpenText Core Application Security での SSO の構成」を参照してください。

DAST: 手動スキャン用のサイト ツリーの可用性

Core Application Securityでは、動的な Web アプリケーションの手動スキャン中に取得されたサイト ツリーにアクセスできるようになりました。この機能により、スキャンされたアプリケーション構造の可視性が向上し、より効果的な分析とレビューが可能になります。サイト ツリー ファイルは、[スキャン] ページから直接ダウンロードできます。

詳細については、『Core Application Security ユーザー ガイド』の「リリース スキャンの表示」を参照してください。

グループ化された手動および自動のDASTの結果

Core Application Securityでは、Dynamic+の検出結果を、手動評価によるものか自動スキャンによるものかによって分類できるようになり、脆弱性がどのように検出されるかについての明確性が向上しました。
詳細については、『Core Application Security ユーザー ガイド』の「リリース スキャンの表示」を参照してください。

セキュリティ標準の更新

Core Application Security は、最新の業界セキュリティ標準を完全にサポートするようになり、プラットフォーム全体におけるレポート作成、分析、ポリシー管理機能が強化されました。
次の標準が全面的にサポート対象となりました。

- DISA STIG 6.4
- CWE Top 25 2025
- OWASP の上位 10 件 2025
- OWASP Top 10 LLM アプリケーション 2025

ユーザー管理のためのAPIキーロール

Core Application Security 26.2では、新しい API キーロール「ユーザー管理」が導入されました。これにより、上位の限を必要とせずに、API ベースでユーザーおよびユーザー グループを管理できるようになります。この新しいロールにより、適切なアクセス制御を維持しながら、ユーザー管理ワークフローをより安全かつ効率的に自動化および統合することが可能になります。

詳細については、『Core Application Security ユーザー ガイド』の「API キー ロール」を参照してください。

システム通知の変更

Core Application Security 26.2 以降、セキュリティ リーダーは、テナントのシングルサインオン (SSO) 設定が変更されるたびに、自動的にメール通知を受け取るようになります。この機能強化により、ID関連の設定変更に対する可視性が向上し、認証設定のタイムリーな把握と管理が確保されます。

開発者の使用権のプロビジョニング

Core Application Security では、開発者ベースのライセンスをサポートするために、[使用権] ページが強化されました。テナント管理者は、テナント設定時に開発者ベースの使用権を構成し、アプリケーションベースのライセンスと並行して管理できます。すべての使用権の種類が単一の統合インターフェイスに表示されるようになり、合計金額の確認、消費量の追跡、可用性の監視、有効期限の詳細の確認が容易になっています。これらの機能強化により、使用権の管理が簡素化され、すべてのライセンスモデルにおいて透明性が向上しています。

詳細については、『Core Application Security ユーザー ガイド』の「使用権の表示」を参照してください。

CycloneDX バージョンのサポート拡張

Core Application Security では、既存の CycloneDX SBOM インポート機能が拡張され、CycloneDX 1.7 仕様に準拠した JSON ファイルにも対応するようになりました。これまでサポートされていたバージョンに変更はなく、今回のアップデートにより最新の CycloneDX 標準との互換性が拡大されています。

詳細については、『Core Application Security ユーザー ガイド』の「ソフトウェア部品表のインポート」を参照してください。

属性設定の強化

属性を設定する際に、[必須] と [セキュリティ リーダーのみが編集可能] を同時に有効にできるようになりました。両方のオプションを選択すると、エンティティ作成時に、属性が適切に設定されるようにするため、システムから既定値が要求されるようになります。[選択リスト] 属性の場合、この既定値は利用可能なリスト値から選択する必要があります。

詳細については、『Core Application Security ユーザー ガイド』の「属性の追加」を参照してください。

MAST+ での追加の資格情報フィールドのサポート

MAST+ のセットアップでは、より高度な認証ワークフローがサポートされるようになりました。MAST+ スキャン時のフォーム認証用に、最大 3 つの資格情報フィールドを追加できます。

詳細については、『Core Application Security ユーザー ガイド』の「モバイル スキャンの構成」を参照してください。

API の更新

OpenText™ Core Application Security API に対し、次の更新が行われました。

- 脆弱性の一括編集エンドポイントが強化され、より広範な更新シナリオに対応できるようになりました。
  - `POST /api/v3/releases/{releaseId}/vulnerabilities/bulk-edit`

  このエンドポイントには、オプションのブール型パラメータ includeAllVulnerabilities が追加されました。これにより、個々の脆弱性や問題 ID を指定することなく、リリースに関連付けられたすべての脆弱性に対して一括更新を適用できます。これにより、大規模な修復アップデートと自動化ワークフローが簡素化されます。

- 以下の属性エンドポイントでは、[必須] と [制限付き] (セキュリティ リーダーのみが編集可能) の両方を同時に有効にできる構成がサポートされるようになりました。
  - `POST /api/v3/attributes`
  - `PUT /api/v3/attributes/{attributeId}`

  この機能強化により、UIベースの属性設定との整合性が確保され、エンティティ作成時の一貫したデータガバナンスが徹底されます。

- 以下の静的スキャンエンドポイントは、AI を活用した SAST をサポートするように機能強化されました。
  - `POST /api/v3/releases/{releaseId}/static-scans/start-scan`
  - `POST /api/v3/releases/{releaseId}/static-scans/start-scan-with-defaults`
  - `POST /api/v3/releases/{releaseId}/static-scans/start-scan-advanced`

  これらのアップデートにより、顧客は、AI を活用した静的解析を、自動化されたパイプラインにシームレスに統合できるようになります。

- 自動化されたデータのエクスポートと処理をサポートする新しいレポート エンドポイントが追加され、ポータルでの手動操作が不要になりました。
  - GET /api/v3/reports/dataexports/templates - 利用可能なデータエクスポートテンプレートを取得します。
  - POST /api/v3/reports/dataexports - 新しいデータエクスポートを開始します。
  - GET /api/v3/reports/dataexports/{dataExportId} - 特定のデータエクスポートのステータスと詳細を取得します

- 開発者ベースのライセンス機能の一環として、以下のエンドポイントで、開発者ベースのライセンス情報の取得がサポートされるようになりました。
  - `GET /api/v3/tenant-entitlements`
  - `GET /api/v3/tenant-open-source-entitlements`

1.4. 既知の問題

PDF 出力に関する問題

説明

Core Application Security の顧客向け PDF ドキュメントには、目的のセクションまたはページに移動しない相互参照リンクが含まれています。ユーザーがこれらのリンクを使用して参照コンテンツにすばやくアクセスするには、場合によってはドキュメント内の情報を手動で見つける必要があります。

回避策

PDF ビューアの検索機能を使用して、参照先のセクションを手動で見つけてください。

ステータス

この問題は調査中です。

For more info, visit https://docs.microfocus.com