OpenText™ Core Application Security

リリース ノート （26.1.0）

Version : 26.1

PDF Generated on : February 12, 2026

Table of Contents

1. リリース ノート （26.1.0）

このドキュメントでは、OpenText™ Core Application Security (Fortify on Demand) リリース 26.1.0 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 26.1.0 には、次のエンジンとルールパックの更新が含まれています。

Fortify Software Security Content 25.4

OpenText Core Application Security は、26.1.0 リリース後に、Fortify Security Research (SSR) の Fortify Software Security Content 25.4 を実装します。詳細については、「Fortify Software Security Content 25.4」を参照してください。

OpenText Static Application Security Testing 25.4

OpenText Core Application Security は、26.1.0 リリース後に、ソース コード スキャン用に OpenText Static Application Security Testing (Fortify Static Code Analyzer) バージョン 25.4 を実装します。

1.3. 新機能

SARIF インポートのサポート

Core Application Security では、SARIF ファイルのインポート、保存、表示をサポートするようになりました。これにより、サードパーティの SAST 結果を統合的に表示できるようになります。*詳細については、『Core Application Security ユーザー ガイド』の「オンプレミス スキャンのインポート」を参照してください。*

Debricked スキャン結果の SPDX SBOM をダウンロード可能

Core Application Security では、既存の CycloneDX 形式に加えて、SPDX SBOM を顧客に公開できるようになりました。この機能を有効にできるように、[**自分のスキャン**]、[**アプリケーション スキャン**]、[**リリース スキャン**] ページの [**SBOM をダウンロード**] オプションを更新して、[**CycloneDX**] と [**SPDX**] という 2 つの形式を用意しました。*詳細については、『Core Application Security ユーザー ガイド』の「すべてのスキャンの表示」、「アプリケーション スキャンの表示」、および「リリース スキャンの表示」を参照してください。*

スキャンへの属性の追加のサポート

お客様がスキャンにカスタム属性 (Git コミット ID、ビルド ID など) を追加できるようになりました。これにより、特定のコード変更や展開の結果の追跡、および CI/CD ワークフローでのスキャンのフィルタリングやレポートが容易になります。*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。*

カスタム属性によるダッシュボードのフィルタリング

FoD をご利用のお客様は、テナントで定義したカスタム属性を使用して、複数のデータ タイプにわたってダッシュボード グラフをフィルタリング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「Magellan ダッシュボード」を参照してください。*

OWASP ASVS 5.0 のサポート

Core Application Security では、新規レポート テンプレート、問題エクスポート列、グループ化とフィルターのオプション、セキュリティ ポリシーの選択などを含め、OWASP ASVS 5.0 が完全にサポートされるようになりました。

修復猶予期間に関する情報を [問題] ページで提供

アプリケーション ポリシーで猶予期間が定義されている場合、開発者は未解決の問題に対する残りの修復猶予期間を確認できるようになりました。この機能強化により、ポリシー違反が発生する前に適切に優先順位を付けて、タイムリーに修復できるようになります。この機能をサポートするために、[**リリースの問題**] および [**アプリケーションの問題**] ページに新しい [**修復猶予期間**] フィールドが追加されました。*詳細については、『Core Application Security ユーザー ガイド』の「アプリケーションの問題の表示」と「リリースの問題の表示」を参照してください。*

監査フィルターによる問題抑制時の監査担当者ステータスの設定機能のサポート

フィルター アクションとして [**抑制**] が選択された場合に、監査テンプレートの設定ページに 2 つ目のドロップダウン リストを表示する機能が追加されました。このドロップダウンでは、問題が抑制されたときに自動的に適用される**監査担当者ステータス**をユーザーが指定できます。*詳細については、『Core Application Security ユーザー ガイド』の「グローバル監査テンプレートの作成」と「アプリケーション監査テンプレートの作成」を参照してください。*

オープンソースの問題に対するファイルの場所に基づいた監査フィルターの作成機能

監査フィルターでは、ファイルの場所に基づいてオープンソースの問題をフィルタリングする機能をサポートするようになりました。この機能を有効にできるように、オープン ソース スキャン タイプに [*ファイルの場所*] 属性が追加されました。*詳細については、『Core Application Security ユーザー ガイド』の「グローバル監査テンプレートの作成」と「アプリケーション監査テンプレートの作成」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。

- SARIF インポート: 新しい API エンドポイント `PUT /api/v3/releases/{releaseId}/static-scans/import-sarif` によって、アプリケーションおよびリリースに対する SARIF ファイルのインポートが可能になりました。
- エンドポイント `GET /api/v3/applications/{applicationId}/users` に、各ユーザーの `accessMethod` の詳細が含まれるようになりました。
- エンドポイント `GET /api/v3/source-scans/{scanId}/sbom` は、**CycloneDX** および **SPDX** SBOM 形式の両方をサポートするように機能強化されました。
- エンドポイント `GET /api/v3/applications/{applicationId}/users` に、電子メール ID、ロール名、およびロール ID が含まれるようになりました。
- Postman API スキャンの設定: エンドポイント `GET /dynamic-scans/scan-setup and PATCH /dynamic-scans/scan-setup/manifest` は、アップロードされたすべて

のファイルと Postman コレクションを返すようになり、複数の Postman ファイル タイプがサポートされるようになりました。

- 脆弱性エンドポイント: エンドポイント `GET /vulnerabilities/{vulnId}/all-data and /vulnerabilities/{vulnId}/details` に、NULL 可能な **remainingRemediationGracePeriodDays** フィールドが含まれるようになりました。

1.4. バグ修正

OpenText Core Application Security 26.1.0 では次の問題が修正されています。

- 以前は、スキャンが完了するとシステムによって生成された電子メールがリリース所有者に届いていました。このスキャン完了時の電子メール通知は送信されなくなりました。

1.5. 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