OpenText™ Core Application Security

リリース ノート （25.4.0）

Version : 25.4

PDF Generated on : November 10, 2025

Table of Contents

1. リリース ノート （25.4.0）

このドキュメントでは、OpenText™ Core Application Security (Fortify on Demand) リリース 25.4.0 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. お知らせ

Core Application Security バージョン 25.4.0:

- ポータル内にある、状況依存のヘルプへのすべてのリンクが機能するようになりました。
- 前評価を要求する会議通話は、モバイルおよび動的セットアップ フォームから廃止されます。この機能は 26.1 以降のバージョンでは利用できなくなります。
- STIG 5.3 に関連するすべての機能は廃止されました。
- 継続的なアプリケーションの監視 (CAM) とその関連機能は完全に廃止され、製品から削除されました。

1.3. 新機能

SAST Aviator: Aviator の監査担当者ステータス マッピングをカスタマイズする機能

25.4.0 以降、監査担当者ステータスはテナント レベルで構成できるようになり、顧客はそれを別個に管理し、誤検知を抑制するかどうかを選択できるようになりました。これをサポートするため、新しいタブである [**SAST Aviator 監査担当者ステータスの構成**] が **[管理] > [設定]** に追加されました。*詳細については、『Core Application Security ユーザー ガイド』の「SAST Aviator 監査担当者ステータスの構成」を参照してください。*

DAST スキャン設定フォームの更新

- 25.4.0 以降、DAST スキャン設定フォームが効率化されました。選択した評価タイプに関連するフィールドのみが表示されるため、動的スキャンをより簡単かつ正確に設定できます。
- 25.4.0 以降では、API スキャン (Postman タイプ) の DAST 設定フォームを使用して、Postman コレクション スキャンを正常に実行するために必要なすべてのファイル タイプをアップロードできます。
  詳細については、『Core Application Security ユーザー ガイド』の「動的スキャンの構成」を参照してください。

モバイル アプリケーション用の SAST スキャン: MBS/Swift/Objective C/C++ テクノロジ スタックの可用性

25.4.0 以降、Core Application Security は、テクノロジ スタック内の Swift、Objective-C、Objective-C++ ファイルに加えて MBS ファイルも受け付けるようになったため、iOS の静的スキャン ワークフローが効率化されます。この機能強化により、ソース コードの送信に必要な macOS スキャナーのみに頼るのではなく、MBS ファイルに Linux を活用できるため、処理コストも低減します。*詳細については、『Core Application Security ユーザー ガイド』の「静的スキャンの構成」を参照してください。*

CSV スキャン データのエクスポート: CSV スキャンのエクスポートでのマイクロサービス名の可用性

25.4.0 以降、顧客は CSV スキャン データのエクスポートでマイクロサービス名を表示できます。*詳細については、『Core Application Security ユーザー ガイド』の「データ エクスポート テンプレートの作成」を参照してください。*

データ エクスポート: スキャンまたは購読の開始日を基準とした使用権の消費データのエクスポートのフィルタリング

25.4.0 以降、Core Application Security では、ユーザーが、選択した期間内での使用権の消費に特に集中できるようになりました。これは、ユーザーが、使用権の消費レポートで期間を選択できるようになったためです。 *詳細については、『Core Application Security ユーザー ガイド』の「データ エクスポート テンプレートの作成」を参照してください。*

インスタンス ID に基づいて問題を検索およびフィルタリングする機能

バージョン 25.4.0 以降、Core Application Security ユーザーは、[アプリケーションの問題] ページと [リリースの問題] ページで、問題をインスタンス ID で検索およびフィルタリングできます。*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概要] ページの操作」と「リリース詳細の表示」を参照してください。*

リリース所有者への通知のオプション化

新しい購読スコープとして、[**所有するすべてのリリース**] が [購読の作成] ページで利用できるようになりました。これにより、リリース所有者は、自分の好みに応じて、自分が作成または所有するすべてのリリースの通知を購読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「独自サブスクリプションの作成」と「グローバル サブスクリプションの作成」を参照してください。*

その他のポータルの更新

DISA STIG 6.3 のサポート

- DISA STIG 6.3 用の新しいレポート モジュールとテンプレートが追加されました。
- 問題データのエクスポートに、DISA STIG 6.3 の列が含まれるようになりました。
- DISA STIG 6.3 が、「アプリケーションの問題」ページと「リリースの問題」ページのグループ化リストとフィルター リストに組み込まれました。
- セキュリティ ポリシーを作成するときに、DISA STIG 6.3 が分類のリストで利用できるようになりました。
- DISA STIG 6.3 が API に追加されました。

API の更新

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

- 顧客は、API を介して、**問題タイプのデータに属性を追加し、値を割り当てる**ことができるようになりました。 `POST /api/v3/releases/{releaseId}/vulnerabilities/bulk-`

`edit` エンドポイントが、`vulnerabilityIds` パラメーターで **GUID と IssueId/Id の両方**を受け入れるように強化されました。

- 顧客は、API を介して、各脆弱性の**最終修正日**の情報を取得できるようになりました。**脆弱性リストを修正日でフィルタリングする**ためのサポートが追加されました。この機能を有効にするため、[**修正日のタイムスタンプ**] フィールドがエンドポイントに追加されています。
  - `GET /api/v3/releases/{releaseId}/vulnerabilities`
- 顧客は、API を介して、**インスタンス ID で問題を検索およびフィルタリングする**ことができるようになりました。この機能をサポートするため、[**インスタンス ID**] フィールドがエンドポイントに追加されています。
  - `GET /api/v3/releases/{releaseId}/vulnerabilities`
- GET /api/v3/releases/{releaseId}/vulnerabilities エンドポイントが更新され、新しいブーリアン フィールドである **`remediationGuidanceAvailable`** が含まれるようになりました。
  - このフィールドに基づいて脆弱性をフィルタリングすることもできます。
- 新しいエンドポイント `GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/aviator-remediation-guidance` が導入されました。
  - これにより、個々の問題に対する機械可読な Aviator の修正の詳細が JSON 形式で返されます。

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