OpenText™ Core Application Security

リリース ノート （25.3.0）

Version : 25.3

PDF Generated on : September 10, 2025

Table of Contents

1. リリース ノート （25.3.0）

このドキュメントでは、OpenText™ Core Application Security (Fortify on Demand) リリース 25.3.0 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 25.3.0:

- SAST Aviator バージョン 25.2.0 が利用可能になりました。
- ScanCentral バージョン 25.2.0 が利用可能になりました。
- OpenText™ Dynamic Application Security Testing (OpenText DAST) バージョン 25.2.0 が利用可能になりました。
- STIG バージョン 5.3 のサポートは廃止される予定です。
- PCI 2.0 DSS コンプライアンスおよび PCI 3.0 DSS コンプライアンスのサポートも廃止される予定です。

1.3. 新機能

新しい DAST 手動評価

25.3.0 以降では、自動スキャナーを使用したスキャンが難しいまたは困難な Web アプリケーションを扱う顧客を支援するために、動的な手動評価機能が提供されます。*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。*

TOTP ベースの 2FA ポータル ログイン

25.3.0 以降、Core Application Security は 2 要素認証 (2FA) の追加オプションとして TOTP をサポートします。詳細については、『Core Application Security ユーザー ガイド』の「ユーザー セキュリティの構成」を参照してください。

SSO の更新

暗号化された SAML アサーションのサポート

Core Application Security では、新しい SAML 暗号化証明書を要求し、それを ID プロバイダ側でのアサーションの暗号化に使用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「暗号化の構成」を参照してください。*

特定のユーザーまたはドメインを SSO の使用から除外する

Core Application Security では、特定のドメインを SSO 構成から除外できるようになりました。テナント内に異なるドメインのユーザーが存在する場合は、SSO ログインの要求から除外するドメインまたはユーザーのリストを指定できます。*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。*

その他のポータルの更新

DISA STIG 6.2、PCI DSS 4.0.1、2024 CWE Top 25 のサポート

Core Application Security は、DISA STIG 6.2、PCI DSS 4.0.1、および 2024 CWE Top 25 標準をサポートするようになりました。ポータルの次の拡張機能が更新されました。

- DISA STIG 6.2、PCI DSS 4.0.1、および 2024 CWE Top 25 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 6.2、PCI DSS 4.0.1、および 2024 CWE Top 25 の列が含まれるようになりました。
- DISA STIG 6.2、PCI DSS 4.0.1、および 2024 CWE Top 25 が、[アプリケーションの問題] ページおよび [リリースの問題] ページのグループ化およびフィルター 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 6.2、PCI DSS 4.0.1、および 2024 CWE Top 25 が分類のリストで利用できるようになりました。
- 脆弱性の詳細を提供する API エンドポイントが更新され、PCI DSS 4.0.1 および 2024 CWE Top 25 の詳細が含まれるようになりました。

[問題] ページでグループ選択から個々の問題を選択解除するオプション

25.3.0 以降では、顧客は [問題] ページで個々の問題を選択解除できます。*詳細については、『Core Application Security ユーザー ガイド』の「リリースの問題の表示」を参照してください。*

[スキャン] ページ: 前回の SAST スキャン以降のペイロードの変更を示す視覚的なキュー

25.3.0 以降では、[スキャン] ページで、現在のスキャンと以前のスキャンのペイロードの差異を表示できます。*詳細については、『Core Application Security ユーザー ガイド』の「すべてのスキャンの表示」を参照してくださ*

い。

[スキャンの概要] ページ: SAST キュー時間の可用性

25.3.0 以降では、顧客は [スキャンの概要] ページでスキャン キュー時間を表示できます。*詳細については、『Core Application Security ユーザー ガイド』の「すべてのスキャンの表示」を参照してください。*

[動的スキャンの設定] フォームの更新

25.3.0 以降では、Core Application Security は、動的+ および DAST 手動評価中のフォーム認証用に 3 つの追加資格情報フィールドをサポートします。*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。*

IP制限の復元

25.3.0 以降では、IP 制限機能が完全に復元されました。詳細については、『Core Application Security ユーザー ガイド』の「ユーザー セキュリティの構成」を参照してください。

Fortify Aviator を SAST Aviator に名前変更

25.3.0 以降では、Aviator 25.2 バージョンは SAST Aviator と呼ばれます。ポータルと製品ドキュメントでも同様の更新が行われます。

Visual Studio Code 修復プラグインへのマーケットプレイス リンク

Visual Studio Code プラグイン修復コードへのリンクが [ツール] ページで利用できるようになりました。

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。

- 履歴エンドポイントにシステム イベントを含めるために、API エンドポイント GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/history に新しい要求パラメーター includeSystemEvents が追加されました。

  既定値は **false** です。値を **false** に設定すると、システム イベントは応答に含まれません。値を **true** に設定すると、システム イベントは応答データにキャプチャされます。

- 次のエンドポイントの機能は、同等の機能を確保するために調整されています。
  - POST/api/v3/releases/{releaseid}/static-scansand start-scan-advanced
  - POST/api/v3/releases/{releaseid}/static-scansand start-scan
- 次の API エンドポイントは、VulnId パラメーターの代わりに VulnId または Id 値を使用するように変更されています。
  - GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId} - 脆弱性のリストを返します
  - GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/all-data - 脆弱性に関するすべてのデータを返します
  - GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/summary - 脆弱性の概要を返します
  - GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/details - 脆弱性の詳細を返します
  - GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/recommendations - 脆弱性に関する推奨事項を返します
  - GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/history - 脆弱性の履歴を返します
  - GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/screenshots - 脆弱性のスクリーンショットを返します
  - GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/screenshot/{screenshotId} – スクリーンショットを返します
  - GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/request-response - 脆弱性の要求と応答を返します

- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/headers - 脆弱性のヘッダーを返します
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/parameters - 脆弱性のパラメーターを返します
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/traces - 脆弱性のトレースを返します
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/traces/{traceIndex}/{traceEntryIndex}/code - 特定のインデックスのトレース コードを返します
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/traces/{traceIndex}/{traceEntryIndex}/snippet - 特定のインデックスのトレース スニペットを返します
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/audit-options - 脆弱性の監査オプションを返します
- GET /api/v3/releases/{releaseId}/vulnerability-filters - 利用可能な脆弱性フィルターを取得します
- GET /api/v3/releases/{releaseId}/vulnerabilities/{vulnId}/comments - 脆弱性の監査コメントを返します

1.4. このリリースでサポートされていない機能

次の機能はサポート対象外になります。

- 2014 より前のバージョンのコンプライアンス レポートは、以下から廃止されます:
  - レポート テンプレートとモジュール
  - データ エクスポート機能
  - [テナントの問題] ページのグループ化とフィルタリング オプション
  - ポリシー マネージャー
  - API
- STIG 5.1 および 5.2 に関連するすべての機能は廃止されます。

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