



リリースノート

Black Duck 2024.7.0

Copyright ©2024 by Black Duck.

All rights reserved.本ドキュメントの使用はすべて、Black Duck Software, Inc.とライセンス所有者間の使用許諾契約に準拠します。本ドキュメントのいかなる部分も、Black Duck Software, Inc.の書面による許諾を受けることなく、どのような形態または手段によっても、複製・譲渡することが禁じられています。

Black Duck、Know Your Code、およびBlack Duckロゴは、米国およびその他の国におけるBlack Duck Software, Inc.の登録商標です。Black Duck Code Center、Black Duck Code Sight、Black Duck Hub、Black Duck Protex、Black Duck Suiteは、Black Duck Software, Inc.の商標です。他の商標および登録商標はすべてそれぞれの所有者が保有しています。

03-10-2024

目次

まえがき.....	6
Black Duck documentation.....	6
カスタマサポート.....	7
Black Duck Software Integrityコミュニティ.....	7
トレーニング.....	7
Black Duck 包括性と多様性に関する声明.....	8
Black Duck セキュリティへの取り組み.....	8
 1. Black Duck 2024.7.0.....	9
発表.....	9
新機能および変更された機能.....	10
APIの機能強化.....	14
バイナリスキャナ情報.....	14
修正された問題.....	14
 2. Previous Releases.....	16
Black Duck 2024.4.x.....	16
Black Duck 2024.4.0.....	16
Black Duck 2024.1.x.....	21
Black Duck 2024.1.1.....	21
Black Duck 2024.1.0.....	24
Black Duck 2023.10.x.....	30
Black Duck バージョン2023.10.2.....	30
Black Duck バージョン2023.10.1.....	31
Black Duck バージョン2023.10.0.....	33
Black Duck 2023.7.x.....	43
Black Duck バージョン2023.7.3.....	43
Black Duck バージョン2023.7.2.....	44
Black Duck バージョン2023.7.1.....	45
Black Duck バージョン2023.7.0.....	50
Black Duck 2023.4.x.....	56
Black Duck バージョン2023.4.2.....	56
Black Duck バージョン2023.4.1.....	57
Black Duck バージョン2023.4.0.....	59
Black Duck 2023.1.x.....	67
Black Duck バージョン2023.1.2.....	67
Black Duck バージョン2023.1.1.....	68
Black Duck バージョン2023.1.0.....	69
Black Duck 2022.10.x.....	75
Black Duck バージョン2022.10.3.....	75
Black Duck バージョン2022.10.2.....	76
Black Duck バージョン2022.10.1.....	77
Black Duck バージョン2022.10.0.....	78
Black Duck 2022.7.x.....	88
バージョン2022.7.2の発表.....	88
バージョン2022.7.2の新機能および変更された機能.....	88

目次

バージョン2022.7.1の発表	88
バージョン2022.7.1の新機能および変更された機能	89
バージョン2022.7.0の発表	91
バージョン2022.7.0の新機能および変更された機能	93
Black Duck 2022.4.x	99
バージョン2022.4.2の新機能および変更された機能	99
バージョン2022.4.1の新機能および変更された機能	99
バージョン2022.4.0の発表	101
バージョン2022.4.0の新機能および変更された機能	105
Black Duck 2022.2.x	110
バージョン2022.2.2の新機能および変更された機能	110
バージョン2022.2.1の新機能および変更された機能	111
バージョン2022.2.0の発表	113
バージョン2022.2.0の新機能および変更された機能	115
Black Duck 2021.10.x	126
バージョン2021.10.3の発表	126
バージョン2021.10.3の新機能および変更された機能	126
バージョン2021.10.2の発表	127
バージョン2021.10.2の新機能および変更された機能	127
バージョン2021.10.1の新機能および変更された機能	128
バージョン2021.10.0の発表	129
バージョン2021.10.0の新機能および変更された機能	131
Black Duck 2021.8.x	136
バージョン2021.8.8の新機能および変更された機能	136
バージョン2021.8.7の発表	137
バージョン2021.8.7の新機能および変更された機能	137
バージョン2021.8.6の発表	138
バージョン2021.8.6の新機能および変更された機能	138
バージョン2021.8.5の新機能および変更された機能	139
バージョン2021.8.4の新機能および変更された機能	140
バージョン2021.8.3の新機能および変更された機能	141
バージョン2021.8.2の新機能および変更された機能	141
バージョン2021.8.1の新機能および変更された機能	142
バージョン2021.8.0の発表	143
バージョン2021.8.0の新機能および変更された機能	144
Black Duck 2021.6.x	149
バージョン2021.6.2の新機能および変更された機能	149
バージョン2021.6.1の新機能および変更された機能	150
バージョン2021.6.0の発表	151
バージョン2021.6.0の新機能および変更された機能	151
Black Duck 2021.4.x	158
バージョン2021.4.1の新機能および変更された機能	158
バージョン2021.4.0の発表	159
バージョン2021.4.0の新機能および変更された機能	160
Black Duck 2021.2.x	167
バージョン2021.2.1の新機能および変更された機能	167
バージョン2021.2.0の発表	167
バージョン2021.2.0の新機能および変更された機能	168
Black Duck 2020.12.x	174
バージョン2020.12.0の発表	174
バージョン2020.12.0の新機能および変更された機能	175
Black Duck 2020.10.x	180
バージョン2020.10.1の新機能および変更された機能	180
バージョン2020.10.0の発表	181

バージョン2020.10.0の新機能および変更された機能.....	181
3. 既知の問題と制限事項.....	189

まえがき

Black Duck documentation

Black Duckのドキュメントは、オンラインヘルプと次のドキュメントで構成されています：

タイトル	ファイル	説明
リリースノート	release_notes.pdf	新機能と改善された機能、解決された問題、現在のリリースおよび以前のリリースの既知の問題に関する情報が記載されています。
Docker Swarmを使用したBlack Duckのインストール	install_swarm.pdf	Docker Swarmを使用したBlack Duckのインストールとアップグレードに関する情報が記載されています。
Kubernetesを使用したBlack Duckのインストール	install_kubernetes.pdf	Kubernetesを使用したBlack Duckのインストールとアップグレードに関する情報が記載されています。
OpenShiftを使用したBlack Duckのインストール	install_openshift.pdf	OpenShiftを使用したBlack Duckのインストールとアップグレードに関する情報が記載されています。
使用する前に	getting_started.pdf	初めて使用するユーザーにBlack Duckの使用法に関する情報を提供します。
スキャンベストプラクティス	scanning_best_practices.pdf	スキャンのベストプラクティスについて説明します。
SDKを使用する前に	getting_started_sdk.pdf	概要およびサンプルのユースケースが記載されています。
レポートデータベース	report_db.pdf	レポートデータベースの使用に関する情報が含まれています。
ユーザーガイド	user_guide.pdf	Black DuckのUI使用に関する情報が含まれています。

KubernetesまたはOpenShiftの環境にBlack Duckソフトウェアをインストールするには、Helmを使用します。次のリンクをクリックすると、マニュアルが表示されます。

- ・ [Helm](#)は、Black Duckのインストールに使用できるKubernetesのパッケージ マネージャです。Black Duck は Helm3をサポートしており、Kubernetesの最小バージョンは1.13です。

Black Duck 統合に関するドキュメントは、次のリンクから入手できます：

- ・ <https://sig-product-docs.synopsys.com/bundle/integrations-detect/page/integrations/integrations.html>
- ・ https://sig-product-docs.synopsys.com/category/cicd_integrations

カスタマサポート

ソフトウェアまたはドキュメントについて問題がある場合は、Black Duckカスタマー サポートに問い合わせてください。

Black Duckサポートには、複数の方法でお問い合わせできます。

- ・ オンライン: <https://www.synopsys.com/software-integrity/support.html>
- ・ 電話: お住まいの地域の電話番号については、[サポートページ](#)の下段にあるお問い合わせのセクションを参照してください。

サポート ケースを開くには、Black Duck Software Integrityコミュニティ サイト(<https://community.synopsys.com/s/contactsupport>)にログインしてください。

常時対応している便利なリソースとして、[オンラインカスタマポータル](#)を利用できます。

Black Duck Software Integrityコミュニティ

Black Duck Software Integrityコミュニティは、カスタマー サポート、ソリューション、情報を提供する主要なオンラインリソースです。コミュニティでは、サポートケースをすばやく簡単に開いて進捗状況を監視したり、重要な製品情報を確認したり、ナレッジベースを検索したり、他のSoftware Integrityグループ (SIG) のお客様から情報を得ることができます。コミュニティセンターには、共同作業に関する次の機能があります。

- ・ つながる – サポートケースを開いて進行状況を監視するとともに、エンジニアリング担当や製品管理担当の支援が必要になる問題を監視します。
- ・ 学ぶ – 他のSIG製品ユーザーの知見とベストプラクティスを通じて、業界をリードするさまざまな企業から貴重な教訓を学ぶことができます。さらに、Customer Hubでは、Black Duckからの最新の製品ニュースやアップデートをいつでもご覧いただけます。これは、当社製品やサービスをより有効に活用し、オープンソースの価値を組織内で最大限に高めることができます。
- ・ 解決する – SIGの専門家やナレッジベースが提供する豊富なコンテンツや製品知識にアクセスして、探している回答をすばやく簡単に得ることができます。
- ・ 共有する – Software Integrityグループのスタッフや他のお客様とのコラボレーションを通じて、クラウドソースソリューションに接続し、製品の方向性について考えを共有できます。

[Customer Successコミュニティにアクセスしましょう](#)。アカウントをお持ちでない場合や、システムへのアクセスに問題がある場合は、[こちら](#)をクリックして開始するか、community.manager@synopsys.comにメールを送信してください。


トレーニング

Black Duck Software Integrityグループ (SIG) は、Black Duckの教育ニーズをすべて満たすワンストップ リソースです。ここでは、オンライントレーニングコースやハウツービデオへの24時間365日のアクセスを利用できます。

新しいビデオやコースが毎月追加されます。

Black Duck Software Integrityグループ (SIG) のCustomer Educationでは、次のことができます。

- ・ 自分のペースで学習する。
- ・ 希望する頻度でコースを復習する。
- ・ 試験を受けて自分のスキルをテストする。
- ・ 終了証明書を印刷して、成績を示す。

詳細については、<https://community.synopsys.com/s/education>でご確認ください。また、Black Duckに関するヘルプについては、ヘルプメニューの[チュートリアル] () (Black DuckのUIに表示)を選択してください。

Black Duck 包括性と多様性に関する声明

Black Duck は、すべての従業員、お客様、パートナー様が歓迎されていると感じられる包括的な環境の構築に取り組んでいます。当社では、製品およびお客様向けのサポート資料から排他的な言葉を確認して削除しています。また、当社の取り組みには、設計および作業環境から偏見のある言葉を取り除く社内イニシアチブも含まれ、これはソフトウェアやIPに組み込まれている言葉も対象になっています。同時に、当社は、能力の異なるさまざまな人々が当社のWebコンテンツおよびソフトウェアアプリケーションを利用できるように取り組んでいます。なお、当社のIPは、排他的な言葉を削除するための現在検討中である業界標準仕様を実装しているため、当社のソフトウェアまたはドキュメントには、非包括的な言葉の例がまだ見つかる場合があります。

Black Duck セキュリティへの取り組み

Black Duckは、お客様のアプリケーションの保護とセキュリティの確保に専念する組織として、お客様のデータ セキュリティとプライバシーにも同様に取り組んでいます。この声明は、Black Duckのお客様と将来のお客様に、当社のシステム、コンプライアンス認証、プロセス、その他のセキュリティ関連活動に関する最新情報をお届けすることを目的としています。

この声明は次の場所で入手できます。[セキュリティへの取り組み | Black Duck](#)

1. Black Duck 2024.7.0

発表

アップグレード後のKnowledgeBaseをアップグレード

Black Duckのアップグレード完了時に、KnowledgeBase更新ジョブが実行されることに注意してください。この更新では、以前のバグに起因する古いKnowledgeBaseコンポーネント ライセンス データを修正するものです。展開の規模にもよりますが、このジョブは最大4時間かかる場合がありますが、通常はそれより短時間で完了します。このプロセスは、スキャンや他のBlack Duckプロセスには影響しません。ただし、このジョブの実行中に、Job runnerポッドのCPUとメモリの使用量が増加していることが観察される場合があります。

アクティビティ監査記録の更新

アクティビティ監査記録機能を使用すると、プロジェクトやプロジェクトのバージョンに影響を与えるアプリケーションのユーザー アクションや主要イベント（プロジェクトのバージョン構成や脆弱性記録など）のアクティビティの監査記録を保持できます。

今回の更新により、パフォーマンスの向上とストレージ コストの削減を目的として、この機能を無効にできるようになりました。これにより、プロジェクトの監査記録に対する柔軟性と制御が向上します。アクティビティ監査記録が無効になっている場合、アクティビティ データは追跡されません。再度有効にすると、その瞬間からアクティビティの追跡が開始されます。

この機能は、新規インストールではデフォルトで無効になっていますが、既存のインストールやアップグレードでは有効のままです。

PostgreSQL 16の外部データベースのサポート

Black Duck は、外部PostgreSQLを使用する新規インストール用にPostgreSQL 16をサポート・推奨するようになりました。ただし、Google CloudSQL for PostgreSQLは、まだ PostgreSQL 16をサポートしていません。そのプラットフォームでは、Black DuckはPostgreSQL 15を推奨しています。

2024.7.xへの移行では、PostgreSQL 16への移行は不要です。

内部PostgreSQLコンテナのユーザーは、アクションは必要ありません。

PostgreSQL 14のサポート終了予定

今後予定している2024.10.0リリースで、Black Duckは外部PostgreSQL 14のサポートを終了します。詳しくは、[「PostgreSQL Version Upgrade Schedule」](#)ページを参照してください。

今後予定しているPostgreSQLコンテナのバージョン15への移行

Black Duck は、2024.10.0リリースでPostgreSQLイメージをバージョン15に移行します。Black DuckのPostgreSQLイメージを使用していないお客様には影響はありません。

今後のPostgreSQLコンテナユーザーに対するアップグレードの制限

Black Duckが提供するPostgreSQLコンテナのユーザーの場合、Black Duck 2024.10.0では、PostgreSQLバージョン13またはPG 14コンテナ(2022.10.0から2024.7.xまで)を使用するBlack Duckの以前のバージョンからの直接アップグレードのみをサポートします。

1. Black Duck 2024.7.0・新機能および変更された機能

(2022.10.0より前の)旧Black Duckバージョンからアップグレードするには、次にある2段階のアップグレードが必要です。

1. Black Duck 2023.7.xにアップグレード。
2. Black Duck 2024.10.xにアップグレード。

今後予定されているWebサーバー テクノロジーの交換

今後のBlack Duckリリース(2024.10.0または2025.1.0)では、既存のIngress Webサーバー(NGiNX)が新しいテクノロジーであるApache APISIXに置き換えられます。既存のカスタムNGiNX構成を使用しているお客様は、互換性を確保するために設定を更新する必要があります。

ドキュメントのローカライゼーション

UI、オンライン ヘルプ、リリース ノートのバージョン2024.4.0が日本語と簡体字中国語にローカライズされました。

2024.7.0以降、日本語と簡体字中国語でローカライズされたドキュメントの更新版は、利用可能になり次第、[Black Duckドキュメント ポータル](#)に掲載されます。

新機能および変更された機能

「新着情報」ウィンドウ

新しい「新着情報」ウィンドウでは、Black Duckの最新リリースで導入された最新機能や拡張機能をご覧いただけます。アップグレード後は、ログイン時に「新着情報」ウィンドウが表示され、このバージョンで最も影響の大きいアップデートは強調表示されます。

ユーザーは以降のログインでこのウィンドウを無効にすることができますが、次にBlack Duck サーバーのアップグレードがあったときは再び表示されます。無効にした場合でも、「新着情報」にはヘルプメニューからアクセスできます。2024.7以降すべてのBlack Duckのメジャー バージョンには、新着情報コンテンツが含まれます。

新しい長期サポート(LTS) 機能

長期サポート(LTS)プロジェクト バージョンは、リリースされた製品バージョンの脆弱性データの追跡を可能にします。LTS プロジェクトは、エンド ユーザーまたは顧客がすでに使用しているソフトウェアを対象としています。LTS プロジェクトはスケーラビリティを念頭に置いて設計されているため、極めて大量のプロジェクト バージョンをサポートできます。

LTS プロジェクト バージョンは、アクティブ プロジェクト バージョンからは最小限のデータを保持し、LTS 部品表(BOM)内のコンポーネントで新たに発見された脆弱性の追跡に重点を置きます。アクティブ バージョンを LTS に変換すると、ソフトウェア部品表(SBOM)が自動的に作成され、必要なサード パーティとの共有が容易になります。LTS バージョンは現在通知機能をサポートしていませんが、Black Duck KnowledgeBase KnowledgeBase に新しい脆弱性データが公開されるとこれを受信します。

新しいAI支援BDSAタグ

AIモデルを使用してBDSAの作成を自動化する新しいメカニズムが導入され、「AI支援」BDSAタグが導入されました。AIツールを使用することで、AI支援Security AdvisoriesはBlack DuckのCyber Security Research Centerで自動で作成されます。これらのBDSAはBDSAチームによって個別に検証されたものではありませんが、自動化されたプロセスと生成AI支援を使用して作成されています。以上のアドバイザリは、Cyber Security Research Centerが識別・検証したBDSAを補完するためのものです。

AI支援タグは、他の脆弱性タグが検出されるすべての領域にあります。

- ・ 脆弱性の[検索]ページのフィルタとして

- ・ プロジェクト バージョンの[セキュリティ]ページのフィルタとして
- ・ ポリシーの脆弱性条件として

内部SSL証明書の新しい有効期限切れアラート

Black Duck 2024.7.0では、内部SSL証明書の新しい有効期限切れアラートが導入されています。このアラートは、内部SSL証明書の有効期限が近づいた際に、30日前にユーザーへ通知します。これにより、タイムリーな更新と中断のない安全な接続が確保されます。

新しいSBOM保持構成

お客様が配布を目的としてSBOMを生成する場合、SBOM管理ソリューションがSBOMを保持し、必要に応じて再作成できるようにすることが重要です。これは他の種類のBlack Duckレポートとは異なり、通常はBOMにこれ以上の変更が予想されない時点でリリースプロセスの一部として発生しますが、常にそうなるとは限りません。

この新機能を使用すると、標準プロジェクトとLTSプロジェクトの両方で、プロジェクト バージョンのSBOMレポートの保持期間を設定できるようになりました。

SBOMの保持設定は、[管理者]→[システム設定]→[データ保持]→[SBOM保持]で設定できます。

SBOMテンプレート内の間接的な依存関係をフィルタ処理する新しいオプション

SBOMテンプレートに、コンポーネントの直接依存関係のみを、または依存関係のないコンポーネントをSBOMに含めるオプションが追加されました。このオプションは、[SBOMテンプレート]ページの[コンポーネント データ]セクション下部にあります。デフォルトの状態はチェックされておらず、CycloneDXとSPDXの両方のレポート タイプに適用されます。チェックを外した場合、構成表内のすべてのコンポーネントが含まれます。

注:この情報は、特定のコンポーネントにのみ利用できる場合があります。

レポートにおける著作権処理の向上

Black Duck 2024.7.0では、SBOMおよび通知ファイル レポートにおける著作権の処理方法が大幅に向上されました。変更内容は次のとおりです。

- ・ 使用されるアルゴリズムの強化により、著作権のリストが作成されます。新しいアルゴリズムでは、これまで見逃されていた著作権が含まれ、コメント文字が削除され、エスケープされた文字コードが実際の文字に置き換えられることで、エントリがより読みやすくなります。
- ・ 著作権リストが英字順にソートされ、リストから重複エントリが削除されました。
- ・ 通知ファイル レポートのカスタマイズ機能を充実させ、ライセンス テキストやライセンス データを除外できるようになりました。通知ファイル レポートには、コンテンツ生成時に選択されたオプションを表示するセクションも追加されました。
- ・ システム設定に新しい著作権ページが追加され、SBOMおよび通知ファイル レポートのグローバルな著作権設定が可能になりました。オプションには、日付が異なる同一の著作権をマージする機能、日付を含まない著作権表示を削除する機能、または標準の著作権タグを使用する機能が含まれます。

通知ファイル レポートの向上

通知ファイル レポートが強化され、ホームページのURLと著作権のないコンポーネントに関する明確な詳細情報が追加されました。2024.7.0より、著作権のないコンポーネントには「著作権が見つかりません」と表示されます。

あいまい一致によるバージョンのないコンポーネントのバイナリ マッチング

バイナリ マッチングにより、バイナリ スキャンからコンポーネントのバージョンを識別する新しい機能がBlack Duckに導入されました。この手法では、バイナリ スキャンに新しいSaaSマッチング サービスが活用され、バイナリ分析で完全一致が見つからない場合、コンポーネント バージョンの最も近い一致または一致するものが特定さ

1. Black Duck 2024.7.0・新機能および変更された機能

れます。このマッチング プロセスは、構成表上で最良の一致をハイライトする方法とともに、継続して行っている KnowledgeBaseの向上の一環として、さらに強化される予定です。

この更新では、あいまい一致APIのサポートも追加されます。あいまい一致のコンポーネント バージョンを利用する バイナリー一致では、それぞれの一致の信頼度と、見つかった代替一致の数が表示されます。

スキャン構成表インポート ログの更新

パフォーマンスの向上とストレージ コストの削減を目的とし、構成表インポート ログを最適化しました。

- ・ 紛失、未発見、またはマッピングされたライセンスの記録は、構成表インポート ログに記録されなくなります。
- ・ 最新の構成表インポート ログのみが保持されます。

これらの向上により、ログ記録プロセスが合理化され、最も関連性の高いデータに焦点を絞ることができ、リソースをより効率的に使用できるようになります。

プロジェクト作成プロセスの更新

プロジェクト作成プロセスは、次のように更新されました。

- ・ サーバー上でSCM統合が有効になっていない場合、[プロジェクトの作成]ボタンをクリックすると、プロジェクト作成フォームが直接表示されます。この状況に変更はありません。
- ・ SCM統合が有効になっている場合、[プロジェクトの作成]ボタンをクリックすると、ドロップダウン メニューに[標準プロジェクト]と[SCMプロジェクト]のオプションが表示されるようになりました。[標準プロジェクト]をクリックすると、プロジェクト作成フォームが表示されます。[SCMプロジェクト]をクリックすると、SCMサーバーの選択ページが表示されます。

[レポート]ビューのcomponent_vulnerabilityテーブルを更新

新しいremediation_updated_atフィールドが、component_vulnerabilityテーブルに追加されました。このフィールドには、脆弱性のトリアージ ステータスが最後に更新された日付が記録されます。

バイナリ スキャンをprotobuf形式に移行

従来のjsonidバイナリ スキャンは、2023.10.0で導入されたプロトコル バッファ形式に移行されました。BDBAを使用するすべてのスキャンが対象になります。この移行により、環境を更新する必要はなく、スキャン結果に影響はありません。

プロジェクト設定とコンポーネントにSBOMフィールドを追加

次のSBOMフィールドが追加されました。

- ・ 発信者: プロジェクト、構成表コンポーネント
- ・ ダウンロード場所: コンポーネント バージョン、カスタム コンポーネント バージョン

署名スキャナにmacOS ARM64サポートを追加

署名スキャナは、macOS ARM64をサポートするようになりました。この更新により、Black Duck製品間の互換性が確保され、ARM64ベースのシステムでパフォーマンスが向上し、シームレスな操作が可能になります。

指定されたポリシー ルール条件の「IN」演算子の削除

次のポリシー ルール条件では、「IN」演算子が許可されなくなりました。この変更は、新規および更新されたポリシー ルールにのみ適用されます。既存のポリシーには影響しません。

- ・ 新規バージョンの数

- ・ 重要度が緊急である脆弱性の数
- ・ 重要度が高である脆弱性の数
- ・ 重要度が中である脆弱性の数
- ・ 重要度が低である脆弱性の数

サポート対象ブラウザのバージョン

- ・ Safariバージョン17.5
 - ・ Safariバージョン14以前はサポートされなくなりました
- ・ Chromeバージョン126.0.6478.127(公式ビルド)(x86_64)
 - ・ Chromeバージョン91以前はサポートされなくなりました
- ・ Firefoxバージョン128.0(64ビット)
 - ・ Firefoxバージョン89以前はサポートされなくなりました
- ・ Microsoft Edgeバージョン 123.0.2420.97(公式ビルド)(64 ビット)
 - ・ Microsoft Edgeバージョン91以前はサポートされなくなりました

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:14-1.25
- ・ blackducksoftware/blackduck-postgres-upgrader:14-1.4
- ・ blackducksoftware/blackduck-postgres-waiter:1.0.13
- ・ blackducksoftware/blackduck-cfssl:1.0.28
- ・ blackducksoftware/blackduck-nginx:2024.7.0
- ・ blackducksoftware/blackduck-logstash:1.0.38
- ・ sigsynopsys/bdba-worker:2024.6.2
- ・ blackducksoftware/rabbitmq:1.2.39
- ・ blackducksoftware/blackduck-authentication:2024.7.0
- ・ blackducksoftware/blackduck-bomengine:2024.7.0
- ・ blackducksoftware/blackduck-documentation:2024.7.0
- ・ blackducksoftware/blackduck-integration:2024.7.0
- ・ blackducksoftware/blackduck-jobrunner:2024.7.0
- ・ blackducksoftware/blackduck-matchengine:2024.7.0
- ・ blackducksoftware/blackduck-redis:2024.7.0
- ・ blackducksoftware/blackduck-registration:2024.7.0
- ・ blackducksoftware/blackduck-scan:2024.7.0
- ・ blackducksoftware/blackduck-storage:2024.7.0
- ・ blackducksoftware/blackduck-webapp:2024.7.0

APIの機能強化

APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

非推奨となった一致したコンポーネントAPIリクエストの削除

2024.7.0リリースで、以下の非推奨APIリクエストが削除されました。

- ・ `/api/projects/{projectId}/versions/{projectVersionId}/matched-components`

vulnerable-bom-componentsの新しいバージョン

次のAPIリクエストの新しいバージョン(V8)が追加されました。

- ・ `/api/projects/<project-id>/versions/<version-id>/vulnerable-bom-components`

このAPIリクエストの最新バージョンでは、パフォーマンスが向上し、出力の品質を向上させるために次の修正が行われています。

- ・ 新しい軽量バージョンでは、vulnerabilityNameとvulnerabilityIdのフィールドが同じ値を持ち、vulnerabilityIdのほうにより一般的に使用されているため、vulnerabilityNameフィールドは`/api/projects/<project-id>/versions/<version-id>/vulnerable-bom-components` APIリクエストから削除されました。

バイナリスキャナ情報

バイナリ スキャナがバージョン2024.6.2に更新されました。

修正された問題

このリリースでは、お客様から報告された次の問題が修正されました。

- ・ (HUB-34550)。Webブラウザのロケールに基づいて、短い数値の日付が表示される方法を修正しました。たとえば、ヨーロッパのロケールでは、日/月/年の日付形式が表示されるようになります。
- ・ (HUB-40168)。著作権表示の問題を修正しました。詳細については、[レポートにおける著作権処理の向上](#)を参照してください。
- ・ (HUB-40687)。検索ページで最後のスキャン時刻が正しく表示されない問題を修正しました。
- ・ (HUB-40774)。CVSS 3の攻撃ベクトル値が「隣接ネットワーク」である脆弱性が、以前はBlack Duckにnull値でマッピングされていた問題を修正しました。2024.7.0現在、値は適切にマッピングされており、キャッシュされた脆弱性でCVSS 3の攻撃ベクトルフィールドがnullになっているものについては、そのデータを埋めるための1回限りのジョブが実行されます。
- ・ (HUB-41220)。[\[検索\]](#)ページで脆弱性を検索した際に、誤った重大度レベルが表示される可能性がある問題を修正しました。
- ・ (HUB-41264)。(一致するスニペットが含まれる)スキャンページと、[\[現在のビューをエクスポート\]](#)ボタンをクリックした際に生成されるCSVファイルで表示されるスキャンサイズが一致しない問題を修正しました。
- ・ (HUB-41348)。スニペットが含まれている場合に、スキャンページでスキャンをサイズで並び替えると正しくない並び替え結果になるという問題を修正しました。
- ・ (HUB-41683)。新しい軽量バージョンでは、vulnerabilityNameとvulnerabilityIdのフィールドが同じ値を持ち、vulnerabilityIdのほうにより一般的に使用されているため、vulnerabilityNameフィールドは`/api/projects/<project-id>/versions/<version-id>/vulnerable-bom-components` APIリクエストから削除しました。

- ・ (HUB-41851)。バージョン詳細レポート(プロジェクトバージョンのアップグレードガイド)の重複した「コンポーネント取得元ID」列の名前をコンポーネント取得元外部IDに変更しました。
- ・ (HUB-42041)。コンポーネントの詳細設定/ライセンス/カスタムフィールドをグローバルレベルで編集した後、Black Duckでアクセスした前のページに戻ろうとすると、ナビゲーションが失われ、二度と戻れなくなるという問題を修正しました。
- ・ (HUB-42054)。`[コンポーネント]`タブで無視された確認済みスニペットのマッチタイプに対し、`/api/projects/{projectId}/versions/{projectVersionId}/risk-profile` APIリクエストが未知のセキュリティリスクを返していた問題を修正しました。
- ・ (HUB-42155)。プロジェクトバージョン自動削除の最終更新日時タイムスタンプが、システムの計算やその他のプロジェクト調整によって誤って変更されるという問題を修正しました。
- ・ (HUB-42225)。プロジェクトバージョンの`[ソース]`タブで、一致しないフィルタオプションで一致しないファイルと一致しないコンポーネントの両方が表示され、その結果から一致しないコンポーネントを見つけにくくなるという問題を修正しました。現在、このフィルタは2つの別々の値に分割されています。一致しないファイル(一致しないファイルのみを表示)と一致しないID(一致しないコンポーネントIDのみを表示)。
- ・ (HUB-42260)。特定の状況下におけるUIおよび脆弱性レポートで、CVE脆弱性の攻撃が利用可能ステータスが一致しない場合がある問題を修正しました。
- ・ (HUB-42363)。プロジェクトに直接/間接的にアクセスできるユーザーがコンテナスキャンのレイヤー情報を参照できないという問題を修正しました。
- ・ (HUB-42402、HUB-42471)。マッピングされたスキャンがないプロジェクトバージョンがプロジェクトバージョンの自動削除にスケジュールされていなかった問題を修正しました。
- ・ (HUB-42466)。パッケージマネージャスキャンで大規模なプロジェクトをスキャンすると、出力ファイルに10,000件を超えるグラフノードが含まれ、最終的にスキャンコンテナがタイムアウトする可能性があるという問題を修正しました。
- ・ (HUB-42478)。hub_db_migrate.shを使用する際、search_pathがレポートデータベースマテビューの定義に正しく渡されないために、レポートデータベースが生成されないという問題を解決しました。
- ・ (HUB-42531)。読み取り専用のYAMLファイルで展開する際にシステムログのダウンロードを試みると、エラー「ログファイルが見つかりません」(Log files not found)が発生する可能性がある問題を修正しました。
- ・ (HUB-42545)。長期サポート(LTS)プロジェクトがプロジェクトバージョンにプロジェクトを追加するモーダルに表示されず、そのためにAPIを手動で呼び出した際にコンポーネントのリストに表示されないという問題を修正しました。
- ・ (HUB-42753)。バイナリー一致によって、構成表一致のAPIで設定されたカウントに余分なIDが誤って追加されるという問題を修正しました。この不一致は一致の信頼度に影響を及ぼし、あいまい一致における選択肢の数と一致しない原因となっていました。
- ・ (HUB-42760)。コンポーネントカテゴリを追加してバージョン詳細レポートを作成すると、スニペットレビューステータス列が欠落するという問題を修正しました。
- ・ (HUB-42811)。vulnerable-bom-components APIエンドポイントのoffset値が、値の設定に関係なく同じ結果を返すというページネーションの問題を修正しました。
- ・ (HUB-42873)。コンポーネントが構成表に存在するかどうかを検証されないために、SBOM著作権レポートが失敗する可能性がある問題を修正しました。
- ・ (HUB-42953)。バージョン詳細レポートのリスクプロファイルで、ライセンス中リスクの数ではなく運用中リスクの数が誤って使用されていた問題を修正しました。
- ・ (HUB-43001)。自動スキャン再試行ヘッダーの構成に関するドキュメントの問題を修正しました。

2. Previous Releases

Black Duck 2024.4.x

Black Duck 2024.4.0

発表

オペレーティング システムのサポート更新

Black Duck 2024.4.0 のインストールに推奨されるオペレーティング システムは次のように更新されました。

- ・ CentOS 7のサポートは終了しました。
- ・ Red Hat Enterprise Linuxサーバー7.9および8.6のサポートは終了しました。
- ・ Red Hat Enterprise Linuxサーバー8.9および9.xのサポートを追加しました。

nginx設定における許可/拒否の廃止と今後予定されている削除

Black Duck 2024.4.0では、blackduck-nginxに組み込まれていた次の機能が非推奨となりました。

- ・ DENY_ACCESS_DIRECTIVES
- ・ ALLOW_ACCESS_DIRECTIVES

これらの機能は、Black Duck 2024.7.0で完全に削除されます。

ドキュメントのローカライゼーション

UI、オンライン ヘルプ、リリース ノートのバージョン2024.1.0が日本語と簡体字中国語にローカライズされました。

新機能および変更された機能

PostgreSQL 16の事前サポート

Black Duck 2024.4.0では、外部データベースとしてPostgreSQL 16を使用できるように事前サポートが追加されました。このサポートはテスト専用です。本番環境での使用はサポートされていません。

新しいReversingLabsマルウェア スキャン

ReversingLabs スキャンを使用すると、ReversingLabsパートナーシップを通じて強化されたマルウェアと脅威のインテリジェンスデータにアクセスできるようになります。ReversingLabsによる複雑なバイナリ解析機能を使用すると、開発者やDevOpsチームは、マルウェア、maldoc、疑わしいファイル、潜在的に望ましくないアプリケーション(PUA)、プロテストウェア、疑わしいファイル構造の異常などの脅威の存在を特定し、危険なソフトウェアサプライチェーン攻撃を回避することができます。

新しいマッチしなかったコンポーネントの自動作成

SBOM管理ワークフローでは、SBOMが入力になります。可視性を失わないためには、KnowledgeBaseとマッチするか否かに関わらず、SBOMに含まれたコンポーネントを全てSBOM管理ソリューション内で永続化する必要があります。この機能は、SBOMにPURLが関連付けられているコンポーネントであれば、SBOMインポートで同名のカスタムコンポーネントを構成表の一致しないコンポーネントとして自動で作成するオプションを提供します。

さらに、SBOMライセンス タグ値がNOASSERTIONの場合、自動作成されたコンポーネントに適用されるデフォルトのライセンスを構成することもできます。

新しいSBOMテンプレート

SBOMテンプレートは、SBOMレポートに含まれる内容を特定する機能を効果的に置き換え、強化する新機能です。SBOMテンプレートでは、生成されたSBOMに含めるフィールドを選択できるほか、(CycloneDX用の)脆弱性情報や開発/ビルド ツールを含めるかどうかなど、その他の設定項目も選択できます。SBOMレポートを作成する際にSBOMテンプレートを選択すると、目的の出力を生成できます。

一部のSBOMフィールド設定がプロジェクト グループ設定からSBOMテンプレート設定に移動されたことに注意してください。Black Duck2024.4.0にアップグレードした後、SBOMレポートを新規生成する前に、SBOMテンプレートをご確認のうえ構成することをお勧めします。

プロジェクト グループ用の新しいCLIコマンド ライン オプションを追加

署名スキャンのコマンド ラインに--project-groupオプションを追加できるようになりました。これにより、プロジェクトを割り当てる「プロジェクト グループ」を設定できます。プロジェクトがまだ存在しない場合は、対応するプロジェクトグループにプロジェクトが新規作成されます。

プロジェクトがすでに存在する場合、または指定したプロジェクトグループが存在しない場合、このパラメータは影響を与えません。

CycloneDX 1.5のサポートを追加

プロジェクトのソフトウェア構成表レポートをCycloneDX v1.5形式でエクスポートできるようになりました。これを行うには、プロジェクト バージョンを表示して[レポート]タブ、[レポートの作成]ボタンの順にクリックし、CycloneDX v1.5 — JSONを選択します。CycloneDX v1.5の詳細については、「[CycloneDX v1.5リファレンス ページ](#)」をご参照ください。

見つからないコンテナのスキャン登録エラー処理の強化

Black Duck登録キーでコンテナ スキャンが有効になっていない場合、コンテナ スキャンは適切なメッセージを表示して失敗します。

SBOMインポート エラー処理の強化

SBOMインポート エラーの処理が向上され、検証に失敗した特定の行/フィールドなど、SBOMインポートが失敗した理由をよりわかりやすく表示できるようになりました。さらに、失敗をログ ファイルにエクスポートして、Black Duck UI外で調査できるようにし、SBOMに必要な更新を行った後に再インポートを試行できるようにできます。

HUB_MAX_MEMORYの設定方法を更新

Black Duck2024.4.0以降、Kubernetesベースの展開では、関連するコンテナに対して構成パラメータHUB_MAX_MEMORYが自動で設定されます。この値は、メモリ制限のパーセンテージとして計算され、90%がデフォルト値です。gen04展開のサイズ設定では、使用される割合を制御するため、hubMaxMemoryがmaxRamPercentageに置き換えられました。この設定の値は、HUB_MAX_MEMORYが以前と同じ値になるように選択されています。

この変更は、Swarmベースの展開には適用されません。

SBOM経由でインポートされたコンポーネントの一致スコアの信頼性を更新

SBOMファイルからコンポーネントがインポートされたプロジェクト バージョンの構成表を表示すると、一致スコアは常に100%と表示され、一致タイプにはSBOMが取得元であることが示されます。

BDBAパッケージ マネージャのサポートによるバイナリ マッチ タイプの結果を更新

以前は、すべてのコンテナおよびバイナリ スキャンで、単一のバイナリ マッチ タイプが生成されていました。BDBAによるパッケージ マネージャのサポートが拡張されたことで、BDBAのマッチング方法に基づく追加のマッチ タイプを特定できるようになりました。その結果、構成表に変更が反映され、バイナリおよびコンテナ スキャンによって識別されたコンポーネントのマッチ タイプが変更されます。

blackduck-webuiコンテナの削除

blackduck-webuiコンテナは削除され、そのビルドはblackduck-nginxコンテナに含まれるようになりました。blackduck-nginxコンテナは、他のblackduckスタックと同じリリース サイクルに従うようになりました。

サポート対象ブラウザのバージョン

- ・ Safariバージョン17.4.1
 - ・ Safariバージョン14以前はサポートされなくなりました
- ・ Chromeバージョン 123.0.6312.124(公式ビルド)(x86_64)
 - ・ Chromeバージョン91以前はサポートされなくなりました
- ・ Firefoxバージョン124.0.2(64 ビット)
 - ・ Firefoxバージョン89以前はサポートされなくなりました
- ・ Microsoft Edgeバージョン 123.0.2420.97(公式ビルド)(64 ビット)
 - ・ Microsoft Edgeバージョン91以前はサポートされなくなりました

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:14-1.22
- ・ blackducksoftware/blackduck-postgres-upgrader:14-1.4
- ・ blackducksoftware/blackduck-postgres-waiter:1.0.12
- ・ blackducksoftware/blackduck-cfssl:1.0.26
- ・ blackducksoftware/blackduck-nginx:2024.4.0-RC
- ・ blackducksoftware/blackduck-logstash:1.0.36
- ・ sigsynopsys/bdba-worker:2024.3.0
- ・ blackducksoftware/rabbitmq:1.2.37
- ・ blackducksoftware/blackduck-authentication:2024.4.0
- ・ blackducksoftware/blackduck-bomengine:2024.4.0
- ・ blackducksoftware/blackduck-documentation:2024.4.0
- ・ blackducksoftware/blackduck-integration:2024.4.0
- ・ blackducksoftware/blackduck-jobrunner:2024.4.0
- ・ blackducksoftware/blackduck-matchengine:2024.4.0
- ・ blackducksoftware/blackduck-redis:2024.4.0
- ・ blackducksoftware/blackduck-registration:2024.4.0
- ・ blackducksoftware/blackduck-scan:2024.4.0
- ・ blackducksoftware/blackduck-storage:2024.4.0

- `blackducksoftware/blackduck-webapp:2024.4.0`

APIの機能強化

APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

SBOM作成者フィールドとSBOM名フィールドに対応した新しいコンポーネント フィルタ キー

構成表コンポーネントのSBOM名と作成者の利用可能な値を返す以下のAPIリクエストに、新しいフィルタ キーが追加されました。

- `GET /api/projects/{projectId}/versions/{projectVersionId}/components-filters`

フィルタ キー:

- `sbomName`
- `sbomCreator`

SBOM作成者フィールドとSBOM名フィールドに対応した新しいコンポーネント フィルタリングのサポート

次のAPIリクエストに新しいフィルタが追加されました。

- `GET /api/projects/{projectId}/versions/{projectVersionId}/components`

フィルタ:

- `sbomName:<File-UUID>`
- `sbomCreator:<Creator-UUID>`

REST APIリクエストに一致する新しいスニペット (生成AIコンプライアンス)

次のAPIリクエストが追加されました。これにより、指定したコード スニペットに一致するスニペットを見つけることができます。

- `POST /api/snippet-matching`

これらの一致は、特定の一致が表すリスクをよりわかりやすく表示するために、ライセンス ファミリごとに並べ替えられています

(`PERMISSIVE`、`WEAK_RECIPROCAL`、`RECIPROCAL`、`RECIPROCAL_AGPL`、`RECIPROCAL_NETWORK`、`UNKNOWN`)。

一致したコンポーネントAPIリクエストの廃止

次の一致したコンポーネントAPIリクエストは非推奨となり、Black Duck 2024.7.0で削除されます。

- `GET /api/projects/{projectId}/versions/{projectVersionId}/matched-components`

バイナリスキャナ情報

バイナリ スキャナがバージョン2024.3.0に更新されました。

修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-39206)。バイナリ スキャナがDEBファイルのコンポーネントを検出せず、結果のレポートにコンポーネントが表示されないという問題を修正しました。
- (HUB-39395)。KnowledgeBaseの更新において、最後に更新したユーザーを、[コンポーネントの管理]でコンポーネントを追加したユーザーとして表示していた問題を修正しました。KnowledgeBaseの更新ジョブで更新されたカスタム コンポーネントは、システム ユーザーとして表示されるようになりました。

- ・ (HUB-39635)。Detect CONTAINER_SCANを他のスキャン タイプ (DETECTORまたはBINARY_SCANなど)と併用して実行した場合に、Detectが想定された412 Precondition Failedエラー メッセージを返さないという問題を修正しました。
- ・ (HUB-40531)。コンポーネント レポートで、一部のコンポーネントについて重複したエントリが作成される可能性がある問題を修正しました。
- ・ (HUB-40745)。構成表に同じコンポーネント バージョンの取得元が複数ある場合に、PackageSupplierフィールドがPurlフィールドの取得元名と異なる場合があるaSPDX SBOMレポートの問題を修正しました。
- ・ (HUB-40769)。次のAPIリクエストは、使用時に404 エラーを返すため非推奨になりました: GET /api/projects/{projectId}/versions/{projectVersionId}/matched-components
- ・ (HUB-40870)。コンポーネントの著作権ページにリンクする「origins-with-filters」リンクの検索パラメータをエンコードするURLを構築する際の問題を修正しました。
- ・ (HUB-40930)。ローカライズされたCSVファイルで、Excelで検索結果を開いた際に文字化けが表示される問題を修正しました。
- ・ (HUB-40998)。ユーザーが削除した際に、SBOMレポートの[パッケージ有効期限]フィールドがクリアされないという問題を修正しました。
- ・ (HUB-41041)。SCAaaS HelmチャートのReadmeファイル内のリンク切れを修正しました。
- ・ (HUB-41063)。同じコンポーネント バージョン内に「推移的」一致と「直接的」一致の両方が存在する場合に「直接的な依存関係」のみが表示されるという問題を修正しました。
- ・ (HUB-41132)。特殊文字「+」を含むコンポーネントを検索すると、期待通りの結果が返されないという問題を修正しました。
- ・ (HUB-41167)。プロジェクト バージョンの一覧表示APIでサポートされているフィルタに関するREST APIのドキュメントを修正しました。サポート対象フィルタは、フェーズ、ライセンス、ディストリビューションのみです。
- ・ (HUB-41276)。不明なライセンスを持つコンポーネントが、通知ファイル レポートに含まれないという問題を修正しました。
- ・ (HUB-41299)。以前にマッピングされ、その後削除されたカスタム コンポーネントが誤って再マッピングされ、その後のスキャンで一致しないコンポーネントの合計に影響を与えていた問題を修正しました。
- ・ (HUB-41316)。SaaSを2023.7.3にアップグレードするとSSOが失敗する可能性がある問題を修正しました。
- ・ (HUB-41318)。コンポーネントのバージョンを検索する際の一貫性のない動作に関する問題を修正しました。
- ・ (HUB-41321)。ZIPファイル内のスニペット結果のコメントがソース レポートにエクスポートされない問題を修正しました。
- ・ (HUB-41362)。検索フィールドに入力されたテキストに基づく検索結果ではなく、すべての検索結果が表示されるという検索フィルタの問題を修正しました。
- ・ (HUB-41365)。/api/projectsの制限が0に設定されている場合 (/api/projects?limit=0)、結果のページが読み込まれないという問題を修正しました。
- ・ (HUB-41369)。アップロードしたブランド ロゴが意図したサイズ要件に合わせて自動で縮小されないという問題を修正しました。
- ・ (HUB-41391)。SBOM内のPURLフィールドが正しく作成されていないために、CycloneDXがSBOMファイルのインポートに失敗する可能性がある問題を修正しました。
- ・ (HUB-41431)。プロジェクト マネージャの役割とプロジェクトの削除権限に関するドキュメントの問題を修正しました。
- ・ (HUB-41450)。deploymentコマンドで、sizing.yamlの前にvalues.yamlファイルを正しく配置するように、readmeファイルを更新しました。

- ・ (HUB-41461)。影響を受けるプロジェクト バージョンの一覧表示APIを使用する際に表示される合計数がプロジェクト バージョンの数ではなく、プロジェクトの数であった問題を修正しました。
- ・ (HUB-41502)。SCAaaSの展開で見えなかったセキュリティの問題を解決しました。
- ・ (HUB-41542)。ファジーBDBAスキャンにおけるkbupdatejobコンポーネントの更新により、構成表の最終更新日がリセットされるという問題を修正しました。
- ・ (HUB-41549)。ユーザー リストをCSV形式でエクスポートする際のローカリゼーションの問題を修正しました。
- ・ (HUB-41552)。プロジェクト バージョンの自動削除機能が無効になってシステムが再起動された場合、プロジェクト バージョンの自動削除機能と、データ保持ポリシーに関係なくプロジェクト バージョンを保持する機能との相互作用に関する問題を修正しました。
- ・ (HUB-41570)。scan_stats_viewマテリアライズド ビューの実行に過度に時間がかかる問題を修正しました。
- ・ (HUB-41591)。HUB CloudSQLデータベースで、deleteクエリによって引き起こされるデッドロックの問題を修正しました。
- ・ (HUB-41773)。フォルダ内の複数のファイルをアップロードしようとして、それらを[SBOM-SPDXファイルのアップロード]または[SBOM-CycloneDXファイルのアップロード]にドラッグした際に発生していた問題を修正しました。
- ・ (HUB-41867)。KB更新ジョブと構成表パッケージ調整(ユーザーが構成表の一致しない外部IDをKBコンポーネントに手動でマッピング)によって生成された脆弱性通知に、イベント ソースが「不明」と誤って表示される問題を修正しました。
- ・ (HUB-41930)。ポッドを実行しているユーザーがroot(0)またはnginx(101)のいずれかでないとnginx Webサーバーが起動しないという問題を修正しました。
- ・ (HUB-41974)。[プロジェクト バージョン] -> [ソース]タブの一致しないフィルタで間違った数が表示される問題を修正しました。
- ・ (HUB-42004)。SSOログイン直後にBlack Duckのページにアクセスすると、意図したページに遷移しないという問題を修正しました。
- ・ (HUB-42051)。UIのコンポーネントのダウンロード場所がクリアされた際に、version_bom_componentのdownload_locationの値が削除されないという問題を修正しました。

Black Duck 2024.1.x

Black Duck 2024.1.1

発表

Black Duck 2024.1.0 Job runnerの問題(HUB-41654)

2024.1.0で、Black Duck Job runnerとKnowledgeBaseの更新チェック ジョブに影響する重大なバグ(HUB-41654)が確認されました。このバグにより、新たな脆弱性または修正された脆弱性を持つ構成表に更新を適用する「KnowledgeBaseデータの更新」ジョブが失敗します。この問題は、特定の脆弱性条件が適用された場合にのみ発生し、影響を受けるのは少数のお客様が使用する構成表のみである可能性が高いです。この問題を解決するため、2024.1.0をご利用のお客様には、2024.1.1へのアップグレードを早急にお勧めします。

この問題は、2024.1.0を使用しているお客様にのみ影響します。詳細については、この問題に関する[コミュニティのお知らせ](#)を参照してください。

新機能および変更された機能

新しいプロジェクト バージョンSBOMフィールド構成

コンポーネントがプロジェクト バージョンのサブプロジェクトとして使用される場合、プロジェクト バージョンのSBOM フィールドを構成して構成表コンポーネントのSBOMフィールドを定義できるようになりました。これにより、サブプロジェクトが使用されるプロジェクトごとにSBOMを定義しなくても、適切な詳細レベルがSBOMに提供されるようになります。

検索機能の更新

Black Duckで検索に使用されるアルゴリズムが強化され、文字列または部分一致を含むすべてのレコードの検索が可能になったことで、必要な情報をより簡単に検索できるようになります。Solr検索で得られる結果と同様の結果が提供されるため、完全な文字列が分からない場合でも関連するレコードを見つけられます。

コンテナバージョン

- blackducksoftware/blackduck-postgres:14-1.21
- blackducksoftware/blackduck-postgres-upgrader:14-1.4
- blackducksoftware/blackduck-postgres-waiter:1.0.11
- blackducksoftware/blackduck-cfssl:1.0.25
- blackducksoftware/blackduck-nginx:2.0.66
- blackducksoftware/blackduck-logstash:1.0.35
- sigsynopsys/bdba-worker:2023.12.3
- blackducksoftware/rabbitmq:1.2.36
- blackducksoftware/blackduck-webui:2024.1.1
- blackducksoftware/blackduck-authentication:2024.1.1
- blackducksoftware/blackduck-bomengine:2024.1.1
- blackducksoftware/blackduck-documentation:2024.1.1
- blackducksoftware/blackduck-integration:2024.1.1
- blackducksoftware/blackduck-jobrunner:2024.1.1
- blackducksoftware/blackduck-matchengine:2024.1.1
- blackducksoftware/blackduck-redis:2024.1.1
- blackducksoftware/blackduck-registration:2024.1.1
- blackducksoftware/blackduck-scan:2024.1.1
- blackducksoftware/blackduck-storage:2024.1.1
- blackducksoftware/blackduck-webapp:2024.1.1

APIの機能強化

プロジェクト バージョンのポリシー ルール概要APIに対する更新

プロジェクト バージョンのポリシー ルール概要APIの新しいバージョンが追加され、ポリシー ルール違反とそれに関連する構成表コンポーネント数の改ページ対応リストが以下の場所に提供されるようになりました。

- `api/projects/{projectId}/versions/{projectVersionId}/policy-rules`

以前のバージョンは非推奨となり、今後のBlack Duckリリースでは削除される予定です。

構成表脆弱性エンドポイントの更新

脆弱性のある構成表コンポーネント エンドポイントに新規バージョン(V8)が追加され、パフォーマンスが向上しました。

・ `/api/projects/{ProjectID}/versions/{VersionID}/vulnerable-bom-components`

バージョン8のエンドポイントには、現在のUI/UXビューやカスタム統合ユーティリティを提供するために最低限のデータのみが含まれており、さらにリアルタイムな結果を生成し、タイムアウト エラーを防止します。このAPIエンドポイントにはV7も存在しており、既存のV6にマッピングされていることに注意してください。

バイナリスキャナ情報

Black Duck 2024.1.1のバイナリ スキャナに関する変更はありません。

修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (HUB-38966)。ポリシー表現が「Newer Versions Count」であるリスクデータの欠落により、ポリシー評価が失敗する可能性がある問題を修正しました。
- ・ (HUB-40443)。UIとレポート間でポリシー違反の相違が発生するアグリゲーター関数の問題を修正しました。
- ・ (HUB-40666)。KbUpdateライセンスジョブの終了時にライセンスの割り当てが更新されない場合がある問題を修正しました。
- ・ (HUB-40690)。Kubernetesで誤った失敗エラーを引き起こす可能性があるrabbitmqの更新で生じる問題を修正しました。
- ・ (HUB-40861)。「ダッシュ」記号とスペースを使用してBlack Duck内のコンポーネントを検索すると、ダブルスペースを入力しないと結果が返されないという問題を修正しました。
- ・ (HUB-40975)。一致しないコンポーネントを一括編集しようとする、エラーメッセージ(アプリケーションに不明なエラーが発生しました)が生成される問題を修正しました。
- ・ (HUB-41054)。プロジェクトバージョンのソースレポートで重複したエントリが出力される問題を修正しました。
- ・ (HUB-41069)。CycloneDX SBOMレポートにSupplierフィールドが表示されない問題を修正しました。
- ・ (HUB-41281)。構成表レポートの[印刷]ボタンをクリックすると、コンポーネントが表示されない問題を修正しました。
- ・ (HUB-41295)。システム管理者以外のユーザーとしてログインした際に、[カスタムフィールドの作成]ページに[作成]ボタンが表示されない問題を修正しました。
- ・ (HUB-41347)。グローバル設定が無効になっている場合でも、バージョン固有のスキャン保持設定が利用可能になっていた問題を修正しました。
- ・ (HUB-41390)。`/api/internal/dashboard-facts` APIリクエストで過剰な数のパラメータが使用された場合にエラーが発生する可能性がある問題を修正しました。
- ・ (HUB-41396)。新たな脆弱性または修正された脆弱性を持つ構成表に更新を適用できないという、「KnowledgeBaseデータの更新」ジョブの失敗の原因となっていた問題を修正しました。詳細については、[関連の発表](#)を参照してください。
- ・ (HUB-41463)。BDDBAワーカログがシステムログから取得されない問題を修正しました。

- ・ (HUB-41502)。セキュリティ上の脆弱性を解決するため、以下のSCAaaSコンポーネントのバージョンを更新しました。

コンポーネント名	旧バージョン	新バージョン
com.fasterxmljackson.core:jackson-core	2.13.3	2.14.1
com.fasterxmljackson.core:jackson-databind	2.13.3	2.13.4.2
com.google.code.findbugs:jsr305	2.0.3	3.0.1
com.google.guava:guava	30.1.1-jre	32.0.1-jre
docker:basejrever	2.0.13	2.0.21
docker:blackducksoftware/hub-docker-common	1.0.6	1.0.7
docker:blackducksoftware/rabbitmq	1.2.32	1.2.36
javax.inject:javax.inject	1	1
javax.validation:validation-api	1.1.0.Final	2.0.1.Final
org.springframework.boot:spring-boot-starter-amqp	2.7.12	2.7.18
org.springframework.boot:spring-boot-starter-hateoas	2.7.12	2.7.18
org.springframework.boot:spring-boot-starter-security	2.7.12	2.7.18
org.springframework.boot:spring-boot-starter-test	2.7.12	2.7.18
org.springframework.boot:spring-boot-starter-web	2.7.12	2.7.18

Black Duck 2024.1.0

発表

upload-cacheサービスの削除

暗号化は、Black Duckのシークレットの暗号化ライブラリとキー ローテーションのメカニズムで処理されるようになりました。この結果、SEAL_KEY変更を処理するrecover_master_key.shおよびbd_get_source_upload_master_key.shスクリプトが削除されました。

また、Black Duckの[ソース]タブで使用する、アップロードしたソース ファイルは移行しません。必要に応じて、既存あるいは新規の一時的なプロジェクトでソースを再スキャンできます。なお、ソースのアップロードは、今後も ENABLE_SOURCE_UPLOADS (デフォルトはfalse) で明示的に有効化される必要があります、MAX_TOTAL_SOURCE_SIZE_MB (デフォルトは4G) とDATA_RETENTION_IN_DAYS (デフォルトは180日) のコンフィグレーション設定を満たすように引き続き自動的に削除されます。

注: デフォルトでは、アップロードされたソース コードは移行しません。なお、移行スクリプトはBlack Duck 2024.1.0リリースの一部としては含まれていません。アップグレードの一環としてアップロードしたソース コードの移行が必要な場合は、Black Duckサポートへお問い合わせください。

スキャンのハードウェア要件の変更

Black Duck 2024.1.0では、数多くの変更がスキャンのハードウェア要件に加えられる予定です。そのため、Black Duckのお客様はご利用の環境を更新し、以下のガイダンスに応じ、追加のハードウェア リソースを必要に応じて割り当てる必要があります。

詳細は[Black Duckハードウェアのスケーリング ガイドライン](#)をご覧ください。

表 1：ハードウェアのスケーリングガイドライン

名前	詳細	
120sph	スキャン／時間: 120 SPH増加率: 0% API／時間: 3,000 プロジェクトバージョン: 13,000	IOPS: 読み取り: 15,000／書き込み: 15,000 Black Duck サービス: CPU: 11コア／メモリ: 56 GB PostgreSQL: CPU: 4コア／メモリ: 16 GB 合計: CPU: 15コア／メモリ: 72 GB
250sph	スキャン／時間: 300 SPH増加率: 20% API／時間: 7,500 プロジェクトバージョン: 15,000	IOPS: 読み取り: 15,000／書き込み: 15,000 Black Duck サービス: CPU: 16コア／メモリ: 86 GB PostgreSQL: CPU: 6コア／メモリ: 24 GB 合計: CPU: 22コア／メモリ: 110 ギガバイト
500sph	スキャン／時間: 650 SPH増加率: 30% API／時間: 18,000 プロジェクトバージョン: 18,000	IOPS: 読み取り: 25,000／書き込み: 25,000 Black Duck サービス: CPU: 23コア／メモリ: 133 GB PostgreSQL: CPU: 16コア／メモリ: 64 GB 合計: CPU: 39コア／メモリ: 197 GB
1,000sph	スキャン／時間: 1,400 SPH増加率: 40% API／時間: 26,000 プロジェクトバージョン: 25,000	IOPS: 読み取り: 25,000／書き込み: 25,000 Black Duck サービス: CPU: 46コア／メモリ: 367 GB PostgreSQL: CPU: 22コア／メモリ: 88 GB 合計: CPU: 68コア／メモリ: 455 GB
1,500sph	スキャン／時間: 1,600 SPH増加率: 6% API／時間: 41,000 プロジェクトバージョン: 28,000	IOPS: 読み取り: 25,000／書き込み: 25,000 Black Duck サービス: CPU: 57コア／メモリ: 459 GB PostgreSQL: CPU: 26コア／メモリ: 104 GB 合計: CPU: 80コア／メモリ: 563 GB
2,000sph	スキャン／時間: 2,300 SPH増加率: 15% API／時間: 50,000 プロジェクトバージョン: 35,000	IOPS: 読み取り: 30,000／書き込み: 30,000 Black Duck サービス: CPU: 64コア／メモリ: 565 GB PostgreSQL: CPU: 32コア／メモリ: 128 GB 合計: CPU: 96コア／メモリ: 693 GB

ドキュメントのローカライゼーション

UI、オンラインヘルプ、およびリリースノートのバージョン2023.10.0が日本語と簡体字中国語にローカライズされました。

新機能および変更された機能

新しいBlack Duck Automated Security Advisories (ASA)

Automated Security Advisories (ASA) は、Black DuckのCyber Security Research Centerが自動化されたAIツールを使用して作成します。ASAは、GitHub Security Advisories (GHSA) フィードのような様々な信頼できるセキュリティフィードと、AIツールを使った自動検証で作成されます。以上のアドバイザリは、[Cyber Security Research Center](#)が識別および検証したBDSAを補完するためのものです。

ASAタグのついたBDSAは、他の脆弱性タグがある全てのエリアにあります。

新しい構成表コンポーネントのダウンロード場所の値

[ダウンロード場所]SBOMフィールドが、[その他のフィールド]のリストに新規追加されました。[ダウンロード場所]は、[構成表コンポーネント]セクションの下にあり、コンポーネントをダウンロードしたバージョン・コントロール・システム (VCS) 内のURLやその他の特定の場所を追加することができます。この新しい情報はSBOMレポートで以下のように表示されます：

- ・ `SPDX:packages > package ID`セクションの下に`downloadLocation`として表示されます。
- ・ `CycloneDX:components > externalReferences`セクションの下に`url`として表示されます。

新しいSBOMレポートの著作権テキスト、ライセンスコメント、ホームページデータ

プロジェクトグループ設定で利用可能なSBOMレポートオプションが更新され、SBOMレポートに著作権データ、ライセンスコメント、ホームページURLを加えることが可能になりました。グループ設定が有効な場合、著作権テキスト、ライセンスコメント、ホームページURLは、CycloneDXとSPDXレポートの両方に含まれます。

新しいSCMリポジトリの自動スキャン

SCMリポジトリ自動スキャンにより、Black DuckはSCMプロジェクトにマッピングされたりリポジトリブランチにおけるコミット、プッシュ、マージなどの変更を毎日チェックし、変更があった場合はスキャンを実行します。この機能を利用するためには、[管理者] → [ジョブ] → [スケジュール済み]で有効化する必要があります。

さらに、以下の機能をサポートするため、Black Duckへ新たにSCMリポジトリ自動スキャン ジョブが2件追加されました:

- ・ **SCMオンボーディングデイリー自動スキャン**: 以前オンボードされたSCMリポジトリの自動スキャンを実行する夜間ジョブをスケジュールします。
- ・ **SCMオンボーディングデイリークリーンアップ**: SCMオンボーディングからクリーンアップする夜間ジョブをスケジュールします。

CISA既知の悪用された脆弱性タグの追加

CISAの既知の悪用された脆弱性カタログに記載された脆弱性について、Black Duckではその旨がタグ付けされるようになりました。これにより、CISA既知の悪用された脆弱性を、脆弱性条件ポリシーのフィルターとして追加できます。詳細は、[CISAの既知の悪用された脆弱性](#)ページをご覧ください。

SCM統合の更新

Black Duck 2024.1.0では、SCM統合のリストに2つの新しいSCMプロバイダが追加されました。

- ・ GitLab SaaS
- ・ Bitbucket

これらの承認済みSCMプロバイダを追加できるようになりました。これらのプロバイダは、追加後、新しいプロジェクトの作成時に選択できます。これを実行すると、新しいプロジェクトの[プロジェクト設定]ページにリポジトリURLとブランチバージョンが自動的に入力されます。

この機能はDetect 8.x以降と互換性があり、新しいパッケージマネージャスキャンで有効になります。

SCM統合はBlack Duckではデフォルトでは有効になっておらず、環境に以下を追加して有効にする必要があります。

Swarmユーザーの場合は、`blackduck-config.env`ファイルに以下を追加します。

```
blackduck.scan.scm.enableIntegration=true
```

Kubernetesユーザーの場合は、`values.yaml`ファイルの`environs`セクションに以下を追加します:

```
environs:
  blackduck.scan.scm.enableIntegration: "true"
```

SBOMレポート関連性情報の更新

SBOMレポートが更新され、依存関係情報が追加されました。SPDXのレポートでは、relationshipsのセクションに依存関係のタイプが含まれるようになりました。適用対象はSPDX 2.3レポートのみであることに注意ください。CycloneDXのレポートには、依存関係のタイプは含まれません。

スニペットコンポーネントマッチに対するディープライセンスデータ管理の更新

ディープライセンスデータ(DLD)とスニペットマッチングを併用するお客様は、コード内のコンポーネントに存在するファイルについて、ディープライセンスリスクを表示するように、プロジェクトを設定できるようになりました。

この機能は、以下の2つで構成されています：

- ・ [ディープライセンスデータを構成表に適用]：このチェックボックスを有効にすると、非スニペットコンポーネントにディープライセンスデータが適用され、宣言されたライセンス以外のコンポーネント内に存在する可能性のある埋め込みライセンスが可視化されます。
- ・ [ディープライセンスデータをスニペットコンポーネントマッチに適用]：有効化された場合、ディープライセンスデータの計算にコンポーネントのスニペットマッチが含まれます。

プロジェクト階層に対するライセンス競合管理の拡張機能

以前は、ライセンスの競合は単一のプロジェクトライセンスからのみ計算され、プロジェクト階層は考慮されていませんでした。Black Duck 2024.1.0では、親プロジェクト内のサブプロジェクトも計算に含まれます。

Black Duck 2024.1.0では、階層的ライセンスの競合はデフォルトで有効になっていますが、お客様の環境で設定可能です。ただし、ライセンス競合情報は自動的に有効になりません。システム管理者は、ライセンス競合を表示するために、[法的小よびライセンス競合]タブを有効にする必要があります。プロジェクトの[設定]タブを使用して、現在のプロジェクトの機能を有効にします。

コンポーネント脆弱性履歴グラフの強化

コンポーネントのページに表示される脆弱性履歴グラフに、未知の取得元の脆弱性データが含まれるようになりました。

SCAに対するKubernetesプローブの強化

Kubernetes環境で使用されるReadiness Probeが以下のように改善されました：

- ・ 新たに追加されたstartupProbeは、コンテナ内のアプリケーションが起動しているかどうかを検証します。startupProbeは、他のどのプローブよりも先に実行され、正常に終了しない限り、他のプローブを無効にします。
- ・ readinessProbeは、30秒の初期遅延(240秒から)の後にチェックを開始し、10秒ごとにチェックします(30秒から)。再起動が実行されるまでに、15回の失敗が許可されます。
- ・ livenessProbesは、10秒ごとにチェックします(30秒から)。
- ・ startupProbeとreadinessProbes用のトグルが新たに追加されました。それぞれのプローブを制御するために固有のフラグが追加されました。

オンデマンドジョブ再試行の強化

これまでのオンデマンドジョブは、最終的に失敗するまでに3回再試行可能でしたが、場合によっては、失敗することがわかっているジョブの再実行が続き、システムリソースを消費する事態につながる可能性があります。このアプローチを改良するため、デフォルトで再試行を無効にし、定期スケジューラが開始したジョブは、対応するチェックジョブが再び実行されたときに再試行するようにしました。

ただし、以上の変更はレポートジョブに影響しませんのでご注意ください。レポートジョブは、通常通り再試行します。

ソースコードのアップロードに関するアップロードキャッシュの変更

注: この変更はBlack Duck 2023.10.0の一部ですが、当時は明確には説明されていませんでした。

Black Duck 2023.4.2では、ソース ファイルをアップロードし、ライセンス検索機能を使用すると、ファイル システムの待ち時間と複数のプロセスが発生するために動作しないという問題に対処するために、AWS上で実行するユーザー向けに回避策が追加されました。

Black Duck 2023.10.0において、この問題は、Black Duckがアップロード キャッシュとストレージ サービスを使用する方法を変更することにより解決しました。アップロード キャッシュは、Black Duckのソース コード アップロード機能では使用されなくなり、ストレージ サービスを介したソース コード アップロードという新しいアーキテクチャ モデルが導入されたことで、根本的な原因が解消しました。

Detect GUI の新リリース

Detect GUIが2024.1.0バージョンに更新され、Black Duck Detect (CLI) 9.1.0バージョンも含まれます。

サポート対象ブラウザのバージョン

- ・ Safariバージョン17.1.2
 - ・ Safariバージョン14以前はサポートされなくなりました
- ・ Chromeバージョン120.0.6099.216 (公式ビルド) (x86_64)
 - ・ Chromeバージョン91以前はサポートされなくなりました
- ・ Firefoxバージョン121.0.1 (64ビット)
 - ・ Firefoxバージョン89以前はサポートされなくなりました
- ・ Microsoft Edge Version 120.0.2210.121 (公式ビルド) (64 ビット)
 - ・ Microsoft Edgeバージョン91以前はサポートされなくなりました

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:14-1.20
- ・ blackducksoftware/blackduck-postgres-upgrader:14-1.3
- ・ blackducksoftware/blackduck-postgres-waiter:1.0.11
- ・ blackducksoftware/blackduck-cfssl:1.0.25
- ・ blackducksoftware/blackduck-nginx:2.0.66
- ・ blackducksoftware/blackduck-logstash:1.0.35
- ・ sigsynopsys/bdba-worker:2023.12.1
- ・ blackducksoftware/rabbitmq:1.2.36
- ・ blackducksoftware/blackduck-webui:2024.1.0
- ・ blackducksoftware/blackduck-authentication:2024.1.0
- ・ blackducksoftware/blackduck-bomengine:2024.1.0
- ・ blackducksoftware/blackduck-documentation:2024.1.0
- ・ blackducksoftware/blackduck-integration:2024.1.0
- ・ blackducksoftware/blackduck-jobrunner:2024.1.0
- ・ blackducksoftware/blackduck-matchengine:2024.1.0

- [blackducksoftware/blackduck-redis:2024.1.0](#)
- [blackducksoftware/blackduck-registration:2024.1.0](#)
- [blackducksoftware/blackduck-scan:2024.1.0](#)
- [blackducksoftware/blackduck-storage:2024.1.0](#)
- [blackducksoftware/blackduck-webapp:2024.1.0](#)

APIの機能強化

Black Duck 2024.1.0には、新規のまたは変更されたAPIリクエストはありません。APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

バイナリスキャナ情報

バイナリスキャナがバージョン2023.12.1に更新されました。

修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-37413)。AzureFileでアップロードソースコードをSCとして使用する際の問題を解決しました。Upload-cacheサービスは完全に削除され、ストレージサービスに置き換えられました。
- (HUB-38991)。コードの場所のサイズを計算する際に、スキャンページの値と矛盾していた問題を修正しました。
- (HUB-39012)。コンポーネントバージョンの承認ステータスを無効な値で更新すると、承認ステータスが「未レビュー」に設定されるREST APIの問題を修正しました。
- (HUB-39160)。URLが操作された場合、プロジェクトのバージョンがプロジェクトの一部であることをBlack Duckが確認していなかった問題を修正しました。今後は、HTTP 404エラーページが返されるようになります。
- (HUB-39361)。タイムスタンプがスキャンテーブルのツールチップとしてのみ表示される問題を修正しました。
- (HUB-39378)。BOMコンポーネントの使用法を編集しても、そのコンポーネントが異なる複数の使用法とマッチしていた場合に無視されることがあった問題を修正しました。
- (HUB-39736)。KB API /component/<uuid>/versionsエンドポイントに関するパフォーマンス上の問題が修正されました。
- (HUB-39864)。BOMコンポーネントの編集で、コンポーネントが1つのマッチに対して複数の取得元を持っていた場合に、複数の取得元が削除される可能性があった問題を修正しました。
- (HUB-39948)。プロジェクトと対応するコードの場所を同時に削除することにより発生する、bomengineのデッドロック問題を修正しました。
- (HUB-39959)。IDP URLまたはXMLに関する検証上の問題が修正されました。IDP検証が失敗した場合、UIは適切なエラーメッセージを表示し、システムは変更されないようになりました。
- (HUB-39983)。リポジトリの再スキャンに失敗すると、Black Duck UIで412エラーが発生する可能性があった問題を修正しました。スキャンのワークフローが改善され、スキャンプロセス中に発生するエラーを処理しやすくなりました。
- (HUB-39987)。[SCMプロジェクトバージョン]で、[最終スキャン日]と[更新日]が空白になっていた問題を修正しました。
- (HUB-40104)。ユーザーの製品登録キーで[暗号文]が登録され、その後登録解除された場合に、コンポーネントの[暗号文]タブが空白のページを表示することがある問題を修正しました。
- (HUB-40667)。概要ダッシュボードのビューで、階層別のプロジェクト・ポリシー違反の情報が入力されない問題を修正しました。
- (HUB-40685)。Detectレート制限パラメータが、Black Duckのドキュメントから欠落していた問題を修正しました。

- ・ (HUB-40898)。最大スニペットファイルサイズが正確な値を表示していなかった、ローカライゼーションの問題を修正しました。

Black Duck 2023.10.x

Black Duck バージョン2023.10.2

- ・ [発表](#)
- ・ [新機能および変更された機能](#)
 - ・ [APIの機能強化](#)
 - ・ [バイナリスキャナ情報](#)
 - ・ [修正された問題](#)

発表

Black Duck 2023.10.2に関する新たな発表はありません。

新機能および変更された機能

Black Duck 2023.10.2には、新機能や変更された機能はありません。

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:14-1.17
- ・ blackducksoftware/blackduck-postgres-upgrader:14-1.2
- ・ blackducksoftware/blackduck-postgres-waiter:1.0.10
- ・ blackducksoftware/blackduck-cfssl:1.0.23
- ・ blackducksoftware/blackduck-nginx:2.0.60
- ・ blackducksoftware/blackduck-logstash:1.0.34
- ・ blackducksoftware/blackduck-upload-cache:1.0.48
- ・ sigsynopsys/bdba-worker:2023.12.0
- ・ blackducksoftware/rabbitmq:1.2.32
- ・ blackducksoftware/blackduck-webui:2023.10.2
- ・ blackducksoftware/blackduck-authentication:2023.10.2
- ・ blackducksoftware/blackduck-bomengine:2023.10.2
- ・ blackducksoftware/blackduck-documentation:2023.10.2
- ・ blackducksoftware/blackduck-integration:2023.10.2
- ・ blackducksoftware/blackduck-jobrunner:2023.10.2
- ・ blackducksoftware/blackduck-matchengine:2023.10.2
- ・ blackducksoftware/blackduck-redis:2023.10.2
- ・ blackducksoftware/blackduck-registration:2023.10.2
- ・ blackducksoftware/blackduck-scan:2023.10.2

- ・ [blackducksoftware/blackduck-storage:2023.10.2](#)
- ・ [blackducksoftware/blackduck-webapp:2023.10.2](#)

APIの機能強化

Black Duck 2023.10.2には、新規のまたは変更されたAPIリクエストはありません。APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

バイナリスキャナ情報

2023.10.2のバイナリスキャナに関する変更はありません。

修正された問題

このリリースでは、次の問題が修正されています：

- ・ (HUB-40763)。SSOページ経由でBlack Duckにログインする際、ユーザーがすぐにログインしない場合、時間が経過すると認証エラーが発生する断続的な問題を修正しました。
- ・ (HUB-40944)。レポートデータベースのコンポーネントテーブルで欠落していたcreated_at および updated_at列を再び追加しました。
- ・ (HUB-40960)。マニフェストファイル内のビルドパッケージがバイナリスキャナーにキャプチャされていた問題を修正しました。

Black Duck バージョン2023.10.1

- ・ [発表](#)
- ・ [新機能および変更された機能](#)
 - ・ [APIの機能強化](#)
 - ・ [バイナリスキャナ情報](#)
 - ・ [修正された問題](#)

発表

ドキュメントのローカライゼーション

オンラインヘルプ、およびリリースノートのバージョン2023.7.0が日本語と簡体字中国語にローカライズされました。

新機能および変更された機能

更新Sigmaバージョン2023.9.0

Sigma 2023.9.0には、Dockerfile のスキャン拡張機能に対する修正が含まれています。

コンテナバージョン

- ・ [blackducksoftware/blackduck-postgres:14-1.17](#)
- ・ [blackducksoftware/blackduck-postgres-upgrader:14-1.2](#)
- ・ [blackducksoftware/blackduck-postgres-waiter:1.0.10](#)
- ・ [blackducksoftware/blackduck-cfssl:1.0.23](#)
- ・ [blackducksoftware/blackduck-nginx:2.0.60](#)
- ・ [blackducksoftware/blackduck-logstash:1.0.34](#)

- [blackducksoftware/blackduck-upload-cache:1.0.48](#)
- [sigsynopsys/bdba-worker:2023.9.4](#)
- [blackducksoftware/rabbitmq:1.2.32](#)
- [blackducksoftware/blackduck-webui:2023.10.1](#)
- [blackducksoftware/blackduck-authentication:2023.10.1](#)
- [blackducksoftware/blackduck-bomengine:2023.10.1](#)
- [blackducksoftware/blackduck-documentation:2023.10.1](#)
- [blackducksoftware/blackduck-integration:2023.10.1](#)
- [blackducksoftware/blackduck-jobrunner:2023.10.1](#)
- [blackducksoftware/blackduck-matchengine:2023.10.1](#)
- [blackducksoftware/blackduck-redis:2023.10.1](#)
- [blackducksoftware/blackduck-registration:2023.10.1](#)
- [blackducksoftware/blackduck-scan:2023.10.1](#)
- [blackducksoftware/blackduck-storage:2023.10.1](#)
- [blackducksoftware/blackduck-webapp:2023.10.1](#)

APIの機能強化

APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

matched-file APIリクエストへのレスポンスの更新

以下のAPIリクエストのレスポンスにuriフィールドが追加されました:

- [/api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/origins/{originId}/matched-files](#)
- [/api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/matched-files](#)
- [/api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/matched-files](#)

バイナリスキャナ情報

2023.10.1のバイナリスキャナに関する変更はありません。

修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-37681)。欠落したパブリックAPI: [api/projects/{projectId}/versions/{versionId}/bom-status/{scanId}](#)がREST API開発者ガイドに追加されました。
- (HUB-39616)。matched-filesクエリに対するAPI応答を更新し、uriフィールドを含めました。詳しくは、「APIの機能強化」セクションを参照してください。
- (HUB-39693)。scan cli使用時のsymlinkに関連するログメッセージをTraceレベルに移動しました。
- (HUB-40316)。ファイル名が空白の場合、スキャンクライアントがBDIOファイルへのデータ書き込みに失敗することがある問題を修正しました。ファイル名が存在し、ヌル文字列でないことを確認するための検証が追加されました。

- ・ (HUB-40354)。サブプロジェクト名とライセンスの取り扱いに関する通知ファイルレポートドキュメントを明確にしました。
- ・ (HUB-40524)。内部ホストオプションのDetect Hosting Locationに関するドキュメントを明確化しました。
- ・ (HUB-40631)。プロジェクトのバージョンがサブプロジェクトとして他のプロジェクトに追加され、サブプロジェクトにニックネームがない場合、バージョン詳細レポートの生成時にNULLポインタ例外が発生することがある問題を修正しました。

Black Duck バージョン2023.10.0

- ・ [発表](#)
- ・ [新機能および変更された機能](#)
 - ・ [APIの機能強化](#)
 - ・ [バイナリスキャナ情報](#)
 - ・ [修正された問題](#)

発表

curlとlibcurlのセキュリティアドバイザリ(CVE-2023-38545、CVE-2023-38546)

Black Duck では、curlとlibcurlに関連するセキュリティ上の問題を認識しています。この問題は、2023年10月3日にプロジェクトのメンテナーと元の作成者によって発見されました。

CVE-2023-38545は、curlバージョン7.69.0～8.3.0(記載バージョンを含む)に影響するもので、curlとlibcurlのコマンドラインツール両方に影響するバッファオーバーフローの脆弱性です。このオーバーフローは、SOCKS5ハンドシェイク中に発生する可能性があります。ハンドシェイクが遅い場合、ユーザーが入力した通常よりも長すぎるホスト名は解決しない可能性があります。そのため、ターゲットバッファへコピーされる可能性があります。そのバッファは割り当てられたサイズを超過する場合があります。このようなヒープベースのバッファオーバーフローは、クラッシュやデータ破損、さらには任意コード実行を招く攻撃として知られています。

CVE-2023-38546はCookieインジェクションの脆弱性に関連します。しかしcurlのメンテナーは、満たす必要がある一連の条件から、悪用される可能性は低いと示唆しています。この脆弱性の影響を受けるバージョンは、7.9.1～8.3.0(記載バージョンを含む)です。curl 8.4.0へアップグレードすると、この問題は解決されます。またユーザーは、curl_easy_duphandle()を呼び出す度に、curl_easy_setopt(cloned_curl, CURLOPT_COOKIELIST, "ALL")を呼び出すことが推奨されます。

当社では、Black Duckの製品、サービス、システムへの露出は限定されていると考えています。当社では露出があった範囲に対し、状況を修正するために最新バージョンのcurlへアップグレードしました。

詳細については、以下をご参照ください。

- ・ [重大なcurlとlibcurlの脆弱性への準備\(CVE-2023-38545\)](#)
- ・ [curlとlibcurlの脆弱性への対処方法](#)

PostgreSQL 14コンテナの移行

Black Duck 2023.10.0では、PostgreSQL 11コンテナを使用するバージョン(バージョン2022.2.0から2022.7.xまで)またはPostgreSQL 13コンテナを使用するバージョン(バージョン2022.10.0から2023.7.xまで)からのアップグレードをサポートしています。インストール中に、blackduck-postgres-upgraderコンテナは既存のデータベースをPostgreSQL 14へ移行し、完了すると終了します。

コア以外のPG拡張機能を使用しているお客様の場合は、移行前にそれらをアンインストールし、移行が正常に完了した後に再インストールすることを強くお勧めします。そうしないと、移行が失敗する可能性があります。

レプリケーションを設定しているお客様は、移行前に、pg_upgradeのドキュメントの手順に従う必要があります。そこで説明されている準備が行われていない場合、移行はおそらく成功しますが、レプリケーションの設定が壊れます。

Black DuckのPostgreSQLイメージを使用していないお客様には影響はありません。

注: 2023.10.0以降、Black Duckでは、PostgreSQL 11またはPostgreSQL 13コンテナを使用するBlack Duckバージョンからの直接アップグレードのみがサポートされるようになります(具体的には、2022.2.0から2023.7.xまでのすべてのBlack Duckバージョン)。古いBlack Duckバージョン(具体的には、2022.2.0より前のすべてのBlack Duckバージョン)からアップグレードするBlack Duck提供のPGコンテナのユーザーは、2023.7.xにアップグレードしてから、2023.10.xにアップグレードするという、2段階アップグレードを行う必要があります。

重要: 移行を開始する前に:

- ・ システムカタログのデータコピーによるディスクの使用に起因する予期しない問題を回避するため、10%ほどの余裕をディスク容量に確保してください。
- ・ ディスク容量が不足するとLinuxシステムが中断する可能性があるため、ルートディレクトリの容量とボリュームマウントを確認してください。

KubernetesおよびOpenShiftユーザーの場合:

- ・ プレーンなKubernetesでは、PostgreSQLポッド内のpostgres-upgrader initコンテナはルートとして実行されます。ただし、唯一の要件は、コンテナがPostgreSQLデータボリュームの所有者と同じUIDで実行されることです。
- ・ OpenShiftでは、postgres-upgrader initコンテナは、PostgreSQLデータボリュームの所有者と同じUIDで実行されることを前提としています。

Swarmユーザーの場合:

- ・ 移行は完全に自動化されているため、Black Duckの標準アップグレードの操作以外に追加の操作は必要ありません。
- ・ blackduck-postgres-upgraderコンテナを、ルートとして実行する必要があります。
- ・ その後のBlack Duckの再起動時に、blackduck-postgres-upgraderは移行が不要であると判断し、すぐに終了します。

PostgreSQL 13のサポートの終了

PostgreSQL 13のサポートは、Black Duck 2023.10.0で終了しました。詳しくは、「[PostgreSQL Version Upgrade Schedule](#)」ページを参照してください。

Black Duckctl利用期間の終了

2023.7.0リリース時点で、Black Duckctlはサポートされなくなり、更新も行われなくなります。Black Duckctlのドキュメントは、<https://github.com/blackducksoftware/hub/tree/master/kubernetes/blackduck>にあります。

この発表は、Black Duck 2023.7.0リリース ノートでは誤って記載漏れされていたことにご注意ください。

PostgreSQLコンテナユーザーに対するアップグレードの制限

Black Duck 2023.10.0では、PostgreSQL 11またはPostgreSQL 13コンテナを使用するBlack Duckバージョンからの直接アップグレードのみがサポートされるようになります(具体的には、2022.2.0から2023.7.x(両端を含む)までのすべてのBlack Duckバージョン)。古いBlack Duckバージョン(具体的には、2022.2.0より前のすべてのBlack Duckバージョン)からアップグレードするBlack Duck提供のPGコンテナのユーザーは、2023.7.xにアップグレードしてから、2023.10.xにアップグレードするという、2段階アップグレードを行う必要があります。

ドキュメントのローカライゼーション

2023.7.0バージョンのUIが日本語と簡体字中国語にローカライズされました。オンラインヘルプとリリースノートのローカライズ版は、今後のリリースで利用できるようになります。

新機能および変更された機能

新しいGitHub SCMリポジトリスキャンと読み取り専用の構成表

Black Duckを、ご利用のGitHubリポジトリに統合できるようになりました。これにより、GitHubにあるすべてのリポジトリ全体を素早く簡単に可視化できるだけでなく、プロジェクト バージョンの構成表としてBlack Duckに追加することも可能になりました。

以下を行えるようになりました。

- ・ 選択したメイン リポジトリを、新しいプロジェクトとしてBlack Duckに追加:これにより、ユーザーはGitHubリポジトリのセキュリティ違反とポリシー違反を素早く表示できます。
- ・ 自由自在にスキャンを実行:リポジトリへマッピングされたBlack Duckバージョン ページからスキャンをトリガーできます。これにより、重大なゼロデイ脆弱性の迅速な検出など、現在のライブラリにおける新しい問題を検出できます。このスキャンの結果、リポジトリの簡単な概要を提供する、読み取り専用のより軽量の構成表が作成されます。この構成表には、検出されたコンポーネントとライセンス、それらのコンポーネントに関連する脆弱性が記載されます。

現在、この機能がサポートされているのは、ホスト型Black Duckのお客様のみであることにご注意ください。SCM統合は、厳格にKubernetes環境内で実行される、ネイティブまたはKubernetes in Docker (KinD)いずれかのサービスを利用します。Black Duckをインストールしてこの機能を使用するには、Helmチャートを使用する必要があります。

新しいスキャンの自動マッピング解除管理ページ

非アクティブなプロジェクトバージョンからスキャンがマッピング解除されるようにスケジュールされるタイミングを、管理できるようになりました。スキャンは、プロジェクトバージョンのフェーズと非アクティブ時間の各条件を満たす必要があり、猶予期間後のみマッピング解除されます。Black Duckで[スキャンの自動マッピング解除]ページを開くには、[管理者ボタン]>[システム設定]>[データ保持]>[スキャンの自動マッピング解除]の順にクリックします。

Black Duck Detectの新しい自動スキャンRetryヘッダーに関するサポート

レート制限スキャンを再試行するタイミングを把握するために、新しいRetry-AfterヘッダーがDetectの429レスポンスに追加されました。以下のプロパティが、blackduck-config.envファイルへ追加されました。

BLACKDUCK_USE_QUEUE_RATE_LIMITING:true を設定し、ご利用の環境下でキューベースのレート制限を有効にします。デフォルト値は、falseです。

BLACKDUCK_INITIAL_RATE_LIMIT_DURATION_BRACKET_THRESHOLD_MINUTES: システムが最初の再試行期間から次の再試行期間へ移行する前に、システムがレート制限を課す必要がある期間を指示します。

BLACKDUCK_RATE_LIMIT_DURATION_THRESHOLD_BRACKET_INCREMENT_MINUTES: システムが次の再試行期間と乗数へ移行する前に、レート制限ブラケットに留まる期間と乗数を指示します。

BLACKDUCK_INITIAL_RETRY_DURATION_MINUTES: 最初のレート制限ブラケットにおける、Retry-Afterヘッダーの最初の期間。

BLACKDUCK_RETRY_DURATION_MULTIPLIER_MINUTES: システムが新しいレート制限期間ブラケットへ達するたびにRetry-After期間に掛ける乗数。

新しいランタイムしきい値環境変数

以下の変数をblackduck-config.envファイルへ追加することで、長時間実行しているジョブを特定するしきい値を設定できるようになりました。

- ・ BLACKDUCK_DEFAULT_JOB_RUNTIME_THRESHOLD_HOURS=[時間単位の値]

この環境変数のデフォルト値は24時間です。

レポートでのサブプロジェクトを含める新しいオプション

以下のレポートを作成する際に、レポート生成ダイアログボックスの新しい[サブプロジェクトを含める]チェックボックスをオンにすることで、サブプロジェクトを含められるようになりました。

- ・ 通知ファイル
- ・ SBOM
- ・ バージョンの詳細

この機能はデフォルトで有効になっていることと、この変更在先立ち、サブプロジェクトはすでにレポート生成に含まれていたことにご注意ください。この機能により、この機能性を明示的に設定できるようになりました。

新しい推移的なアップグレードガイダンス

この機能はBlack Duck 2023.1.0で追加されましたが、同バージョンのリリース ノートでは誤って記載漏れしていたことにご注意ください。

セキュリティリスクを解決する最も簡単な方法は、使用されているコンポーネントを、より脆弱性の少ないバージョンにアップグレードすることです。直接的マッチとして使用されているコンポーネントに対して、より簡単に実施できます。推移的な依存関係によってもたらされるコンポーネントの脆弱性の軽減や除去は、そのコンポーネントにもたらされる根本的な直接的依存関係を理解していないと、より困難になります。この機能の目標は、推移的なアップグレードガイダンスをより簡単かつ直接的に提供し、より優れた開発者体験とより明確な行動喚起を実現することです。

Black Duckセキュア コンテナ(BDSC)の強化

Black Duck では、新しい種類のコンテナ イメージ スキャンとプロジェクト ビューが導入されました。これにより、コンテナ イメージ由来のリスクの管理を簡素化できます。コンテナプロジェクトでは集約された構成表とリスクを表示できるだけでなく、リスクをレイヤーごとに表示する方法も提供されます。これには、リスクを基本イメージやOS、アプリケーションの各レイヤーから分けて表示する機能も含まれます。また、コンポーネントがレイヤーのどこにいつ追加／削除されたかを表示するサポートも追加されました。

加えて、Black Duck KnowledgeBaseのインベントリが拡大し、Docker Hubのベース コンテナ イメージとレイヤーごとのコンポーネントの詳細が範囲に含まれるようになったことで、Black Duckがクライアント コンテナのスキャンに集中できるようになります。

署名スキャン、バイナリ スキャン、Docker Inspectorの一環としての既存のBlack Duckコンテナ イメージ スキャンには変更はなく、引き続きサポートされます。新しいコンテナイメージスキャンの機能とプロジェクトビューにより、コンテナで検出されるリスクの管理に関するユーザー体験が向上するため、お客様はコンテナレイヤーごとにリスクを管理できるようになります。

この機能を活用するには、ご利用の製品登録キーでBlack Duck Secure Container (BDSC)を有効にする必要があります。Black Duck Binary Analysis統合型サブスクリプションのお客様は、本機能がライセンスに含まれます。

ライセンスリスクの集約を強化 – 限られたお客様が使用可能

この機能強化の前は、サブプロジェクト由来のライセンスリスクは追跡されておらず、親プロジェクト内で表示することもできませんでした。つまり、サブプロジェクト階層の使用時に、ライセンスリスクを見落とす可能性があることを示していました。現在ではこの機能を有効にすると、プロジェクトの構成表にあるサブプロジェクトに表示されるライセンスリスクは、サブプロジェクトのライセンスリスクとそのコンポーネントの最高のライセンスリスクに応じて判断されるようになりました。

この機能は一般利用できず、デフォルトでは有効になっていないことにご注意ください。強化されたライセンス リスクの集約は、次のBlack Duckリリースで一般利用できるようになります。その際に、デフォルトで有効になります。

SBOMインポートコンポーネントの可視性を強化

SBOMのインポートの結果として生成されたコンポーネントを、その他のタイプの特定／スキャンまたはその他のインポートされたSBOMによるものと区別して特定する機能が導入されました。プロジェクトバージョンのソースタブで、SBOMタイプ（SPDXまたはCycloneDX）、SBOMがインポートされたタイミング、SBOMの提供者、SBOMの作成に使用されたツールのバージョンなどの情報を特定できます。

コンポーネントバージョンページの強化

コンポーネントバージョンページでは、システム管理者が設定した評価システムの優先度に基づくセキュリティリスクの範囲まで、ユーザーが探している内容をより明確に表示できるようになりました。表には、コンポーネントバージョンにその他の脆弱性があるかどうかや、CVSS v2などの他の評価システムではどれくらいの脆弱性があるかが示されるようになりました。

ジョブページ機能の強化

ジョブページの処理タブで、通常よりも長時間実行されているジョブの隣に警告アイコンが表示されるようになりました。また、このページを長時間実行されているジョブでフィルタリングし、これらのジョブのリストを表示できます。

また、新しいPrometheusメトリックを利用できるようになりました。これにより、ユーザーはシステムで通常よりも長時間実行されているジョブを確認できます。

スキャンのハードウェア要件の変更

Black Duck 2023.10.0では、数多くの変更がスキャンのハードウェア要件に加えられています。そのため、Black Duckのお客様はご利用の環境を更新し、以下のガイダンスに応じ、追加のハードウェア リソースを必要に応じて割り当てなければなりません。「[Black Duckハードウェアのスケールング ガイドライン](#)」をご参照のうえ、これらの推奨事項へ変更が加えられた際に備え、最新情報をご確認ください。

表 2：ハードウェアのスケールングガイドライン

名前	詳細	
10sph	スキャン／時間：50 SPH増加率：400% API／時間：2,500 プロジェクトバージョン：10,000	IOPS：読み取り：15,000／書き込み：9,000 Black Duck サービス：CPU：10コア／メモリ：36 GB PostgreSQL：CPU：2コア／メモリ：8 GB 合計：CPU：12コア／メモリ：44 GB
120sph	スキャン／時間：120 SPH増加率：0% API／時間：3,000 プロジェクトバージョン：13,000	IOPS：読み取り：15,000／書き込み：15,000 Black Duck サービス：CPU：11コア／メモリ：56 GB PostgreSQL：CPU：4コア／メモリ：16 GB 合計：CPU：15コア／メモリ：72 GB
250sph	スキャン／時間：300 SPH増加率：20% API／時間：7,500 プロジェクトバージョン：15,000	IOPS：読み取り：15,000／書き込み：15,000 Black Duck サービス：CPU：16コア／メモリ：85 GB PostgreSQL：CPU：6コア／メモリ：24 GB 合計：CPU：22コア／メモリ：109 GB
500sph	スキャン／時間：650 SPH増加率：30% API／時間：18,000 プロジェクトバージョン：18,000	IOPS：読み取り：25,000／書き込み：25,000 Black Duck サービス：CPU：23コア／メモリ：133 GB PostgreSQL：CPU：16コア／メモリ：64 GB 合計：CPU：39コア／メモリ：197 GB
1,000sph	スキャン／時間：1,400 SPH増加率：40% API／時間：26,000 プロジェクトバージョン：25,000	IOPS：読み取り：25,000／書き込み：25,000 Black Duck サービス：CPU：44コア／メモリ：367 GB PostgreSQL：CPU：22コア／メモリ：88 GB 合計：CPU：66コア／メモリ：455 GB

名前	詳細
1,500sph	スキャン／時間: 1,600 SPH増加率: 6% API／時間: 41,000 プロジェクトバージョン: 28,000 IOPS: 読み取り: 25,000／書き込み: 25,000 Black Duck サービス: CPU: 53コア／メモリ: 464 GB PostgreSQL: CPU: 26コア／メモリ: 104 GB 合計: CPU: 79コア／メモリ: 568 GB
2,000sph	スキャン／時間: 2,300 SPH増加率: 15% API／時間: 50,000 プロジェクトバージョン: 35,000 IOPS: 読み取り: 30,000／書き込み: 30,000 Black Duck サービス: CPU: 64コア／メモリ: 565 GB PostgreSQL: CPU: 32コア／メモリ: 128 GB 合計: CPU: 96コア／メモリ: 693 GB

表 3 : PostgreSQLの設定

名前	詳細
10sph	スキャン／時間: 50 PostgreSQL CPU／メモリ: 2コア／メモリ: 8 GB shared_buffers (MB): 2,654 effective_cache_size (MB): 3,185 autovacuum_max_workers: 4 maintenance_work_mem (MB): 512 max_connections: 400 work_mem (MB): 50
120sph	スキャン／時間: 120 PostgreSQL CPU／メモリ: CPU: 4コア／メモリ: 16 GB shared_buffers (MB): 5,336 effective_cache_size (MB): 6,404 autovacuum_max_workers: 4 maintenance_work_mem (MB): 512 max_connections: 400 work_mem (MB): 50
250sph	スキャン／時間: 300 PostgreSQL CPU／メモリ: CPU: 6コア／メモリ: 24 GB shared_buffers (MB): 8,016 effective_cache_size (MB): 9,619 autovacuum_max_workers: 6 maintenance_work_mem (MB): 1,024 max_connections: 500 work_mem (MB): 35
500sph	スキャン／時間: 650 PostgreSQL CPU／メモリ: CPU: 16コア／メモリ: 64 GB shared_buffers (MB): 21,439 effective_cache_size (MB): 25,727 autovacuum_max_workers: 6 maintenance_work_mem (MB): 1,024 max_connections: 500 work_mem (MB): 35
1,000sph	スキャン／時間: 1,400 PostgreSQL CPU／メモリ: CPU: 22コア／メモリ: 88 GB shared_buffers (MB): 29,502 effective_cache_size (MB): 35,403 autovacuum_max_workers: 6 maintenance_work_mem (MB): 2,048 max_connections: 600 work_mem (MB): 48
1,500sph	スキャン／時間: 1,600 PostgreSQL CPU／メモリ: 26コア／メモリ: 104 GB shared_buffers (MB): 34,878 effective_cache_size (MB): 41,854 autovacuum_max_workers: 8 maintenance_work_mem (MB): 4,096 max_connections: 800 work_mem (MB): 58
2,000sph	スキャン／時間: 2,300 PostgreSQL CPU／メモリ: 32コア／メモリ: 128 GB shared_buffers (MB): 42,974 effective_cache_size (MB): 51,569 autovacuum_max_workers: 8 maintenance_work_mem (MB): 4,096 max_connections: 800 work_mem (MB): 58

アーカイブされたプロジェクトバージョンフェーズのポリシー評価を更新

以下の変更が、アーカイブされたプロジェクトバージョンフェーズに加えられました。

- ・ プロジェクトバージョンフェーズのポリシー式は「Archived」を値として許可しなくなった
- ・ プロジェクトバージョンフェーズと「Archived」値を含む既存のポリシールールは、自動で無効になる
- ・ 新しいポリシールールと式の変更は、「Archived」フェーズのプロジェクトバージョンで評価されなくなった

PostgreSQL設定の更新

Black Duck 2023.10.0以降、PostgreSQLコンテナを使用する導入では、PostgreSQLの設定は自動で設定されます。外部PostgreSQLを使用するお客様は、設定を引き続き手動で適用する必要があります。

Black Duckホスト型Detectバージョンの更新

Black Duck 2023.10.0では、Black Duck Detect 9のサポートをBlack Duck Detectページで提供するようになり、Detect 7.xのサポートは終了しました。Black Duck 2023.10.0へアップグレードした後、Detect 7.xを現在ご利用のお客様には、Detect 7.xのサポートが終了したため、アップグレードが推奨されている旨を伝える警告インジケータが表示されます。この構成の変更後は、Detect 7.xへ戻せなくなることにご注意ください。

ArtifactoryとSCM統合の要件を更新

ArtifactoryとSCM統合をお客様の環境で使用するには、お使いの登録キーでこれらの機能を有効にする必要があります。有効にしたら、以下をvalues.yamlファイルに追加する必要があります。

```
enableIntegration: true
```

SCA as a Service導入ファイルの更新

以下のように、SCA as a Serviceに使用する導入ファイルが更新されました。

- ・ RabbitMQイメージを1.2.14から1.2.29へ更新
- ・ 適切な通信のため、ポートを構成するための以下の新しい環境変数を追加:
 - ・ BLACKDUCK_RABBIT_LISTENERS_PORT: "5672"
 - ・ BLACKDUCK_RABBIT_MANAGEMENT_PORT: "15672"

マッチしないコンポーネントを表示機能の更新

「マッチしないコンポーネント」数をプロジェクトバージョンコンポーネントビューに表示するかどうかを判断するために使用される、BLACKDUCK_HUB_SHOW_UNMATCHEDプロパティがデフォルトで有効になりました。

この変更はBlack Duck 2023.7.0で加えられましたが、同バージョンのリリース ノートでは誤って記載漏れされていたことにご注意ください。

SBOMフィールドの監査記録を更新

プロジェクトのアクティビティタブで、以下のSBOMフィールドへの追加や変更が報告されるようになりました。

- ・ パッケージサプライヤ名
- ・ パッケージサプライヤのメールアドレス
- ・ パッケージサプライヤのタイプ

レポートデータベーステーブルの更新

以下のテーブルが更新されました。

- created_at列がcomponent_policiesテーブルへ追加されました。この列には、ポリシー違反が作成されたタイミングのリストが含まれます。
- purl列がcomponentテーブルへ追加されました。この列には、コンポーネントのパッケージURLが含まれます。

レポートデータベースの更新

レポートデータベースのコンポーネントテーブルからも、APIを介して取得したchannel_release_external_namespaceとして保存されている詳細が利用できるようになりました。このテーブルには、取得元の一般的な名前空間（Maven、Debian、Ubuntuなど）が記載されています。

ログインページとフレームの更新

Black Duck周辺のログイン ページとフレームが更新されました。

コンテナスキャン機能の名前を更新

Black Duck「Container Scanning — 限られたお客様が使用可能」の名前が、Black Duck Secure Container (BDSC) へと変更されました。Black Duck Secure Containerのスキャンでは、コンテナイメージ、そのレイヤー、ベースイメージ内のコンポーネントを特定する機能を提供します。

この更新に応じ、製品登録ページも更新されました。

Kubernetesのデフォルトのストレージサービスサイズを増加

Black Duck 2023.10.0では、コンテナ サイズとJavaヒープ サイズが1 GBストレージ/512 MBメモリから2 GBストレージ/1 GBメモリへと増加しました。

コンテナバージョン

- blackducksoftware/blackduck-postgres:14-1.16
- blackducksoftware/blackduck-postgres-upgrader:14-1.1
- blackducksoftware/blackduck-postgres-waiter:1.0.10
- blackducksoftware/blackduck-cfssl:1.0.23
- blackducksoftware/blackduck-nginx:2.0.60
- blackducksoftware/blackduck-logstash:1.0.34
- blackducksoftware/blackduck-upload-cache:1.0.48
- sigsynopsys/bdba-worker:2023.9.4
- blackducksoftware/rabbitmq:1.2.32
- blackducksoftware/blackduck-webui:2023.10.0
- blackducksoftware/blackduck-authentication:2023.10.0
- blackducksoftware/blackduck-bomengine:2023.10.0
- blackducksoftware/blackduck-documentation:2023.10.0
- blackducksoftware/blackduck-integration:2023.10.0
- blackducksoftware/blackduck-jobrunner:2023.10.0

- blackducksoftware/blackduck-matchengine:2023.10.0
- blackducksoftware/blackduck-redis:2023.10.0
- blackducksoftware/blackduck-registration:2023.10.0
- blackducksoftware/blackduck-scan:2023.10.0
- blackducksoftware/blackduck-storage:2023.10.0
- blackducksoftware/blackduck-webapp:2023.10.0

APIの機能強化

REST APIリクエストのページナビゲーションを強化

ページ化された結果を返していたREST APIは、データを反復処理できるようにするため、同じシーケンスにあるその他のページへのリンクを提供するようになりました。

GET /api/jobs-runtimesリクエストの更新

ジョブが長時間実行されているかどうかを判断する値を、GET /api/jobs-runtimesレスポンスに含めるようになりました。

```
"longRunningThresholdMs" : 3300,
"longRunning" : false
```

longRunningThresholdMs値は、ジョブのタイプに対するランタイムしきい値を判断します。ジョブがこの制限を超えると、長時間実行されているジョブとして見なされます。longRunning値は、対象のジョブのランタイムと前回実行時の期間に基づき、そのジョブが長時間実行されているかどうかを判断します。

/api/projectリクエストのパフォーマンスを向上

以下のAPIリクエストのパフォーマンスが向上しました。

- /api/projects/{project id}
- /api/projects/{project id}/versions/{version id}/components
- /api/projects/{project id}/versions

バイナリスキャナ情報

バイナリスキャナがバージョン2023.9.3に更新されました。

- コンテナスキャンをサポートするようになりました。

修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-27209)。CVSS 2.0スコアがない脆弱性が原因で、KB更新ジョブが失敗する可能性がある問題が修正されました。
- (HUB-32753)。アップロードキャッシュのクリーニングで、古いDocker Inspectorのアップロードを処理しなかった問題を修正しました。
- (HUB-33560)。アーカイブ済みプロジェクトフェーズのポリシールールを無効にしました。違反していたすべてのコンポーネントはクリアされます(アーカイブ済みプロジェクトバージョン内のものも含む)。新しいポリシールールは、「アーカイブ済み」プロジェクトバージョンに対しては評価されません。式の変更は、「アーカイブ済み」プロジェクトバージョンに対しては評価されません。無効化・削除されたポリシールールは、「アーカイブ済み」プロジェクトバージョンからクリアされます。

- ・ (HUB-35760)。[スキャン]ページの[完了]フィルタで、現在進行中のスキャンが誤って表示されていた問題が修正されました。
- ・ (HUB-35836)。プロジェクトへのその他の直接アクセス権を何も持たないユーザーが、プロジェクト所有者ユーザーを削除でき、それによって直接アクセス権を持たないユーザーをプロジェクトのプロジェクトマネージャの役割に割り当てることができた問題が修正されました。修正後、プロジェクトへの直接アクセス権を持たないユーザーは、そのプロジェクトからユーザーを削除しようとしてもブロックされるようになりました。
- ・ (HUB-38385、HUB-38654)。スキャンの処理における従来の方法に関連する、タイムアウトの問題が修正されました。
- ・ (HUB-38595)。REST API開発者ガイドに記載されている、GET /api/codelocations/{codeLocationId}/latest-scan-summaryリクエストのレスポンス例が更新されました。
- ・ (HUB-38682)。[ソース]列の下にある構成表ビューの「N個のマッチ」リンクをクリックしても、[ソース]タブの以前の選択がクリアされず、以前にマッチしたフォルダ／ファイルが表示されていた問題が修正されました。
- ・ (HUB-38753)。コンポーネントバージョンの使用の一括編集が、ポリシー違反の更新に誤って失敗する可能性があった問題が修正されました。
- ・ (HUB-38766)。プロジェクトビューアユーザーがプロジェクトの設定ページにアクセスし、プロジェクトへ更新を加えることができた問題を修正しました。この修正により、権限のないプロジェクトビューアユーザーはプロジェクト設定ページへ引き続きアクセスできるものの、何も更新できないようになりました。すべての更新／削除アクションは無効になります。
- ・ (HUB-38803)。構成表ページの[未確認のスニペット]リンクをクリックすると、無視としてマークされたスニペットが依然として表示されていた問題が修正されました。このリンクをクリックすると、[マッチを無視: 無視しない]フィルタがスニペットページへ自動で適用されるようになりました。
- ・ (HUB-38806)。APIの脆弱性を介するBDSA-2023-1225の修正で、HTTP 404エラーが生成される可能性があった問題が修正されました。
- ・ (HUB-38841)。[コンポーネントライセンス]モーダルに記載されている、ライセンスの注記と属性ステートメントのテキストサイズが修正されました。
- ・ (HUB-38878)。コンポーネントのマージが発生すると、コンポーネントが構成表から削除される可能性があった問題が修正されました。
- ・ (HUB-39079)。大規模なHTMLレポートのレンダリングを試みると、「HTTP 503 Service Unavailable (HTTP 503 サービスは利用できません)」サーバーエラーレスポンスが生成される可能性があった問題が修正されました。修正後は、大規模なHTMLレポートのレンダリングを試みると、実際のレポートサイズと現在のサイズ制限が記載された検証エラーを生成するようになりました。現在のサイズ制限は、HUB_MAX_HTML_REPORT_SIZE_KB環境変数によって判断されます。デフォルトでは3,000 KBIに設定されています。
- ・ (HUB-39275)。マップされていないスキャンの保持がUIで365日間を超える期間に設定されていた場合、ページジョブが実行された際にその日数が30日間にリセットされていた問題が修正されました。
- ・ (HUB-39318)。特定のコンポーネントのバージョンの[著作権]タブにある取得元を強調表示できなかった問題が修正されました。
- ・ (HUB-39368)。ユーザーがその他のタブをクリックすると、グローバル検索が現在選択している検索のクエリを上書きしていた問題が修正されました。修正後、検索リクエストは保持されなくなりました。つまり、ユーザーがブラウザの更新やログアウトして再ログインを行うと、以前のフィルタは記憶されません。
- ・ (HUB-39441)。初期化時に、ScmServerAppServiceがSCM統合の登録キーしかチェックしない問題が修正されました。
- ・ (HUB-39496)。BDASキャンから生成されたBDIOのファイル サイズが16 GBを超えると、Black Duckへのアップロードに失敗する可能性があった問題が修正されました。サイズ制限は90 GBに増加されました。
- ・ (HUB-39744)。KBUpdateWorkflowJobの実行後に、構成表／バージョンページとダッシュボードに表示される脆弱性の結果に不一致が生じていた問題が修正されました。

- ・ (HUB-39836)。component_matchesマテリアライズドビューに含まれないマッチタイプがあった問題が修正されました。
- ・ (HUB-39864)。複数の取得元(カーソルを移動して表示)を含む構成表コンポーネントの編集(使用法やコメントの変更)により、すべての取得元が削除される可能性があった問題が修正されました。
- ・ (HUB-40060)。多くの取得元を含むコンポーネントを構成表で編集する際に、選択できる取得元が10個に限られていた問題が修正されました。100個選択できるようになりました。
- ・ (HUB-40085)。レポート作成時、生成に予想以上の時間が掛かり、パイプラインの待機時間が発生する可能性があるというパフォーマンスの問題が修正されました。

Black Duck 2023.7.x

Black Duck バージョン2023.7.3

- ・ [発表](#)
- ・ [新機能および変更された機能](#)
 - ・ [APIの機能強化](#)
 - ・ [バイナリスキャナ情報](#)
 - ・ [修正された問題](#)

発表

curlとlibcurlのセキュリティアドバイザリ(CVE-2023-38545、CVE-2023-38546)

Black Duck では、curlとlibcurlに関連するセキュリティ上の問題を認識しています。この問題は、2023年10月3日にプロジェクトのメンテナーと元の作成者によって発見されました。

CVE-2023-38545は、curlバージョン7.69.0～8.3.0(記載バージョンを含む)に影響するもので、curlとlibcurlのコマンドラインツール両方に影響するバッファオーバーフローの脆弱性です。このオーバーフローは、SOCKS5ハンドシェイク中に発生する可能性があります。ハンドシェイクが遅い場合、ユーザーが入力した通常よりも長すぎるホスト名は解決しない可能性があります。そのため、ターゲットバッファへコピーされる可能性があります。そのバッファは割り当てられたサイズを超過する場合があります。このようなヒープベースのバッファオーバーフローは、クラッシュやデータ破損、さらには任意コード実行を招く攻撃として知られています。

CVE-2023-38546はCookieインジェクションの脆弱性に関連します。しかしcurlのメンテナーは、満たす必要がある一連の条件から、悪用される可能性は低いと示唆しています。この脆弱性の影響を受けるバージョンは、7.9.1～8.3.0(記載バージョンを含む)です。curl 8.4.0へアップグレードすると、この問題は解決されます。またユーザーは、curl_easy_duphandle()を呼び出す度に、curl_easy_setopt(cloned_curl, CURLOPT_COOKIELIST, "ALL")を呼び出すことが推奨されます。

当社では、Black Duckの製品、サービス、システムへの露出は限定されていると考えています。当社では露出があった範囲に対し、状況を修正するために最新バージョンのcurlへアップグレードしました。

詳細については、以下をご参照ください。

- ・ [重大なcurlとlibcurlの脆弱性への準備\(CVE-2023-38545\)](#)
- ・ [curlとlibcurlの脆弱性への対処方法](#)

新機能および変更された機能

コンテナバージョン

注: nginx v2.0.61とupload-cache v1.0.49のイメージは、curlの脆弱性に対応するために2023.7.3専用に作成されたもので、いずれも2023.7.3でのみ展開する必要があります。いずれも、Black Duck 2023.10.0との互換性はありません。

- blackducksoftware/blackduck-postgres:13-2.29
- blackducksoftware/blackduck-authentication:2023.7.3
- blackducksoftware/blackduck-webapp:2023.7.3
- blackducksoftware/blackduck-scan:2023.7.3
- blackducksoftware/blackduck-jobrunner:2023.7.3
- blackducksoftware/blackduck-cfssl:1.0.23
- blackducksoftware/blackduck-logstash:1.0.34
- blackducksoftware/blackduck-registration:2023.7.3
- blackducksoftware/blackduck-nginx:2.0.61
- blackducksoftware/blackduck-documentation:2023.7.3
- blackducksoftware/blackduck-upload-cache:1.0.49
- blackducksoftware/blackduck-redis:2023.7.3
- blackducksoftware/blackduck-bomengine:2023.7.3
- blackducksoftware/blackduck-matchengine:2023.7.3
- blackducksoftware/blackduck-webui:2023.7.3
- blackducksoftware/blackduck-storage:2023.7.3
- sigsynopsys/bdba-worker:2023.9.3
- blackducksoftware/rabbitmq:1.2.32

APIの機能強化

Black Duck 2023.7.3には、新規のまたは変更されたAPIリクエストはありません。APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

バイナリスキャナ情報

2023.7.3のバイナリスキャナに関する変更はありません。

修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-40080)。reporting.component_vulnerabilityビューを更新するためのマテリアライズドビューの更新クエリが、複数の異なるReportingDatabaseTransferJobから並行して複数回実行される可能性があった問題が修正されました。

Black Duck バージョン2023.7.2

- [発表](#)

- ・ [新機能および変更された機能](#)
 - ・ [APIの機能強化](#)
 - ・ [バイナリスキャナ情報](#)
 - ・ [修正された問題](#)

発表

Black Duck 2023.7.2に関する新たな発表はありません。

新機能および変更された機能

Black Duck 2023.7.2には、新機能や変更された機能はありません。

APIの機能強化

Black Duck 2023.7.2には、新規のまたは変更されたAPIリクエストはありません。APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

バイナリスキャナ情報

2023.7.2のバイナリスキャナに関する変更はありません。

修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (HUB-39559)。毎回のサーバー起動時に、暗号化キーのローテーションが誤ってトリガーされていた問題が修正されました。また、SAML秘密キーが暗号化キーのローテーションに含まれていなかった問題も修正されました。

Black Duck バージョン2023.7.1

- ・ [発表](#)
- ・ [新機能および変更された機能](#)
 - ・ [APIの機能強化](#)
 - ・ [バイナリスキャナ情報](#)
 - ・ [修正された問題](#)

発表

今後のスキヤンのハードウェア要件に関連する変更

Black Duck 2023.10.0では、数多くの変更がスキヤンのハードウェア要件に加えられる予定です。そのため、Black Duckのお客様はご利用の環境を更新し、以下のガイダンスに応じ、追加のハードウェア リソースを必要に応じて割り当てる必要があります。

表 4：ハードウェアのスケーリングガイドライン

名前	詳細	
10sph	スキヤン／時間: 50 SPH増加率: 400% API／時間: 2,500 プロジェクトバージョン: 10,000	IOPS: 読み取り: 15,000／書き込み: 9,000 Black Duck サービス: CPU: 10コア／メモリ: 36 GB PostgreSQL: CPU: 2コア／メモリ: 8 GB 合計: CPU: 12コア／メモリ: 44 GB

名前	詳細	
120sph	スキャン／時間: 120 SPH増加率: 0% API／時間: 3,000 プロジェクトバージョン: 13,000	IOPS: 読み取り: 15,000／書き込み: 15,000 Black Duck サービス: CPU: 11コア／メモリ: 56 GB PostgreSQL: CPU: 4コア／メモリ: 16 GB 合計: CPU: 15コア／メモリ: 72 GB
250sph	スキャン／時間: 300 SPH増加率: 20% API／時間: 7,500 プロジェクトバージョン: 15,000	IOPS: 読み取り: 15,000／書き込み: 15,000 Black Duck サービス: CPU: 16コア／メモリ: 85 GB PostgreSQL: CPU: 6コア／メモリ: 24 GB 合計: CPU: 22コア／メモリ: 109 GB
500sph	スキャン／時間: 650 SPH増加率: 30% API／時間: 18,000 プロジェクトバージョン: 18,000	IOPS: 読み取り: 25,000／書き込み: 25,000 Black Duck サービス: CPU: 23コア／メモリ: 133 GB PostgreSQL: CPU: 16コア／メモリ: 64 GB 合計: CPU: 39コア／メモリ: 197 GB
1,000sph	スキャン／時間: 1,400 SPH増加率: 40% API／時間: 26,000 プロジェクトバージョン: 25,000	IOPS: 読み取り: 25,000／書き込み: 25,000 Black Duck サービス: CPU: 44コア／メモリ: 367 GB PostgreSQL: CPU: 22コア／メモリ: 88 GB 合計: CPU: 66コア／メモリ: 455 GB
1,500sph	スキャン／時間: 1,600 SPH増加率: 6% API／時間: 41,000 プロジェクトバージョン: 28,000	IOPS: 読み取り: 25,000／書き込み: 25,000 Black Duck サービス: CPU: 53コア／メモリ: 464 GB PostgreSQL: CPU: 26コア／メモリ: 104 GB 合計: CPU: 79コア／メモリ: 568 GB
2,000sph	スキャン／時間: 2,300 SPH増加率: 15% API／時間: 50,000 プロジェクトバージョン: 35,000	IOPS: 読み取り: 30,000／書き込み: 30,000 Black Duck サービス: CPU: 64コア／メモリ: 565 GB PostgreSQL: CPU: 32コア／メモリ: 128 GB 合計: CPU: 96コア／メモリ: 693 GB

表 5 : PostgreSQLの設定

名前	詳細	
10sph	スキャン／時間: 50 PostgreSQL CPU／メモリ: 2コア／メモリ: 8 GB shared_buffers (MB): 2,654 effective_cache_size (MB): 3,185	autovacuum_max_workers: 4 maintenance_work_mem (MB): 512 max_connections: 400 work_mem (MB): 50
120sph	スキャン／時間: 120 PostgreSQL CPU／メモリ: CPU: 4コア／メモリ: 16 GB shared_buffers (MB): 5,336 effective_cache_size (MB): 6,404	autovacuum_max_workers: 4 maintenance_work_mem (MB): 512 max_connections: 400 work_mem (MB): 50
250sph	スキャン／時間: 300 PostgreSQL CPU／メモリ: CPU: 6コア／メモリ: 24 GB shared_buffers (MB): 8,016 effective_cache_size (MB): 9,619	autovacuum_max_workers: 6 maintenance_work_mem (MB): 1,024 max_connections: 500 work_mem (MB): 35
500sph	スキャン／時間: 650 PostgreSQL CPU／メモリ: CPU: 16コア／メモリ: 64 GB shared_buffers (MB): 21,439	autovacuum_max_workers: 6 maintenance_work_mem (MB): 1,024 max_connections: 500 work_mem (MB): 35

名前	詳細	
	effective_cache_size (MB) : 25,727	
1,000sph	スキャン／時間 : 1,400 PostgreSQL CPU／メモリ : CPU : 22コア／メモリ : 88 GB shared_buffers (MB) : 29,502 effective_cache_size (MB) : 35,403	autovacuum_max_workers: 6 maintenance_work_mem (MB) : 2,048 max_connections: 600 work_mem (MB) : 48
1,500sph	スキャン／時間 : 1,600 PostgreSQL CPU／メモリ : 26コア／メモリ : 104 GB shared_buffers (MB) : 34,878 effective_cache_size (MB) : 41,854	autovacuum_max_workers: 8 maintenance_work_mem (MB) : 4,096 max_connections: 800 work_mem (MB) : 58
2,000sph	スキャン／時間 : 2,300 PostgreSQL CPU／メモリ : 32コア／メモリ : 128 GB shared_buffers (MB) : 42,974 effective_cache_size (MB) : 51,569	autovacuum_max_workers: 8 maintenance_work_mem (MB) : 4,096 max_connections: 800 work_mem (MB) : 58

新機能および変更された機能

新しいArtifactory構成管理

Artifactory Integration構成を、Black Duck UI内で管理できるようになりました。これを行うには、統合マネージャユーザーとしてログインし、[管理者]ボタンをクリックして、[統合]を選択します。

これにより、多くの環境プロパティが削除され、Black Duck UIで構成可能になりました。以下のプロパティは削除されました。

- BLACKDUCK_SCAAAS_ARTIFACTORY_ANNOTATE_VIOLATING_POLICY_RULES
- BLACKDUCK_SCAAAS_ARTIFACTORY_EXCLUDE_FILETYPES
- BLACKDUCK_SCAAAS_ARTIFACTORY_HOST
- BLACKDUCK_SCAAAS_ARTIFACTORY_IGNORE_SSL
- BLACKDUCK_SCAAAS_ARTIFACTORY_INCLUDE_FILETYPES
- BLACKDUCK_SCAAAS_ARTIFACTORY_PORT
- BLACKDUCK_SCAAAS_ARTIFACTORY_REPOSITORIES
- BLACKDUCK_SCAAAS_ARTIFACTORY_DOCKER_REPOSITORIES
- BLACKDUCK_SCAAAS_ARTIFACTORY_SCAN_REPORT_ENABLED
- BLACKDUCK_SCAAAS_ARTIFACTORY_SCAN_REPORT_REPOSITORY
- BLACKDUCK_SCAAAS_ARTIFACTORY_SCHEME
- BLACKDUCK_SCAAAS_ARTIFACTORY_SEARCHER_ADAPTIVE_QUEUE
- BLACKDUCK_SCAAAS_ARTIFACTORY_SEARCHER_QUEUE_SIZE
- BLACKDUCK_SCAAAS_ARTIFACTORY_SEARCHER_SCHEDULE_DELAY
- BLACKDUCK_SCAAAS_ARTIFACTORY_TOKEN
- BLACKDUCK_SCAAAS_ARTIFACTORY_UPDATED_WINDOW_HOURS

- ・ BLACKDUCK_SCAAAS_ARTIFACTORY_URI_PATHBLACKDUCK_SCAAAS_FAILED_COUNT
- ・ BLACKDUCK_SCAAAS_FAILED_TIMEOUT_HOURS
- ・ BLACKDUCK_SCAAAS_MANAGER_SEARCHER_QUEUE_THRESHOLD_HIGH
- ・ BLACKDUCK_SCAAAS_MANAGER_SEARCHER_QUEUE_THRESHOLD_LOW
- ・ BLACKDUCK_SCAAAS_PROCESSING_TIMEOUT_HOURS
- ・ BLACKDUCK_SCAAAS_SEARCHER_CUTOFF_DATE
- ・ BLACKDUCK_SCAAAS_REPOSITORY_TYPE

Artifactory Integrationサービスの新しいDockerイメージ／コンテナ

Artifactory Integration と併用できる新しいDockerイメージ／コンテナが追加されました。ホスト型Black Duckのお客様は、このイメージ／コンテナの展開前に、お使いの登録キーでArtifactory Integrationを有効にする必要があります。

Artifactory Integrationの新しいSCAエンジンプロパティ

Black Duckとsca-engine-as-a-serviceを相互通信させるには、以下のenviromsプロパティをBlack Duckのvalues.yamlファイルへ追加する必要があります。

```
BLACKDUCK_SCA_ENGINE_SCHEME:  
BLACKDUCK_SCA_ENGINE_HOST:  
BLACKDUCK_SCA_ENGINE_PORT:
```

注: 上記のプロパティをvalues.yamlファイルへ追加する必要があるものの、その値を直ちに設定する必要はなく、上記の例のように空欄のままにできます。sca-engine-as-a-serviceの導入へ付ける予定の名前に基づき、BLACKDUCK_SCA_ENGINE_HOSTの値は変更されます。

新しいユーザーの役割

以下の新しいユーザーの役割が、役割全体のリストへ追加されました。

- ・ 統合マネージャ: この役割は、すべての統合を管理することを可能にします。
- ・ 軽量構成表コードスキャナ: この役割は、軽量構成表への管理者権限を付与します。
- ・ 軽量構成表プロジェクトマネージャ: この役割は、軽量構成表プロジェクトへの管理者権限を付与します。
- ・ 軽量構成表プロジェクトバージョンマネージャ: この役割は、軽量構成表プロジェクトバージョンへの管理者権限を付与します。

フルスニペットスキャン機能の更新

スニペットスキャンの使用量の増加に伴い、スニペットスキャンのパフォーマンスとスケーラビリティに関する問題が見られるようになりつつあります。これらの問題を軽減するため、以下の戦術的な制限と最適化を導入しています。これにより、スニペットを管理し、スニペットマッチングの冗長なリワークを削減することが可能になります。

- ・ スニペットファイルサイズの最大許容範囲を(1~16 MBから)1~4 MBへ削減
- ・ スニペットファイルサイズの最大デフォルト値を(2 MBから)1 MBへ変更

また、お使いの登録キーでフルスニペットスキャンオプションをアクティブ化することを必須としました。影響を受ける検出パラメータは、以下になります。

[detect.blackduck.signature.scanner.snippet.matching](#)

- ・ FULL_SNIPPET_MATCHING

- FULL_SNIPPET_MATCHING_ONLY

コンテナバージョン

- blackducksoftware/blackduck-postgres:13-2.27
- blackducksoftware/blackduck-authentication:2023.7.1
- blackducksoftware/blackduck-webapp:2023.7.1
- blackducksoftware/blackduck-scan:2023.7.1
- blackducksoftware/blackduck-jobrunner:2023.7.1
- blackducksoftware/blackduck-cfssl:1.0.20
- blackducksoftware/blackduck-logstash:1.0.32
- blackducksoftware/blackduck-registration:2023.7.1
- blackducksoftware/blackduck-nginx:2.0.47
- blackducksoftware/blackduck-documentation:2023.7.1
- blackducksoftware/blackduck-upload-cache:1.0.45
- blackducksoftware/blackduck-redis:2023.7.1
- blackducksoftware/blackduck-bomengine:2023.7.1
- blackducksoftware/blackduck-matchengine:2023.7.1
- blackducksoftware/blackduck-webui:2023.7.1
- blackducksoftware/blackduck-storage:2023.7.1
- sigsynopsys/bdba-worker:2023.6.0
- blackducksoftware/rabbitmq:1.2.28

APIの機能強化

APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

pURL APIリクエストを介した、新しいコンポーネントのメタデータ検索

パッケージURLを検索語句として使用することで、単一のコンポーネントの検索に以下のAPIリクエストを使用できます。レスポンスでは、コンポーネント、バージョン、バリエーションに関する詳細情報を取得するためのエンドポイントが提供されます。

- GET /api/search/kb-purl-component

コンポーネントのAPIエンドポイントレスポンスを更新

以下に記載されたコンポーネントのAPIエンドポイントのレスポンスを更新し、リクエストで使用するbomMatchInclusionフィルタオプション(trueまたはfalse)を含めました。

- /api/projects/{projectId}/versions/{projectVersionId}/components

バイナリスキナ情報

2023.7.1のバイナリスキナに関する変更はありません。

修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (HUB-38374)。リポジトリのプルを試みる際に異なる日時形式を使用するとエラーが発生する可能性があった、Black Duck SCM統合の問題が修正されました。
- ・ (HUB-38790)。一部の移行スクリプトで構文エラーが発生していた問題が修正されました。
- ・ (HUB-38968)。名前空間のUUID値がSBOMのベスト プラクティスに従っていないため、SBOMのBlack Duckへのアップロードが失敗する可能性があった問題が修正されました。
- ・ (HUB-39026)。Detect 8が実行された、またはBDIO集約が使用された際に、マッチしないコンポーネントのバッジ(現在はデフォルトで有効)が、パッケージファイルを誤って集計していた問題が修正されました。この問題により、BDIOファイルの階層が原因で、実行されているパッケージマネージャの数が、マッチしないコンポーネント数に追加されていました。
- ・ (HUB-39072)。REST APIドキュメントに記載されている、構成表コンポーネントの脆弱性修正の表記に関するCreatedAt定義とUpdatedAt定義を、それぞれ脆弱性が構成表コンポーネントの取得元へ追加された日付、および脆弱性が構成表コンポーネントの取得元で更新された日付であると記載するように修正しました。
- ・ (HUB-39168)。変更されたコンポーネントで、「フィルタの追加」と「フィルタのバージョン...」の各テキストフィールドオプションが表示されない可能性があり、コンポーネントが変更された場合に脆弱性の履歴グラフが表示されない可能性があるUIの問題が修正されました。
- ・ (HUB-39211)。日本語ローカライゼーションで、ポリシー上書き日付情報が正しく表示されていなかった問題が修正されました。
- ・ (HUB-39274)。KbUpdateJobで、お客様の製品登録からBDSAのライセンス付与を検証していなかった問題が修正されました。この問題により、リクエスト中にHTTP 403 Forbiddenレスポンスが発生する可能性があります。
- ・ (HUB-39367)。""を含むライセンス名が原因で、KbUpdateWorkflowJob-License Updateが失敗する可能性があった問題が修正されました。

Black Duck バージョン2023.7.0

- ・ [発表](#)
- ・ [新機能および変更された機能](#)
 - ・ [APIの機能強化](#)
 - ・ [バイナリスキャナ情報](#)
 - ・ [修正された問題](#)

発表

Docker 18.09.xおよび19.03.xのサポート終了。

Black Duck 2023.7.0で、Docker 18.09.xおよび19.03.xのサポートは終了しました。サポートされるバージョンはDocker 20.10.xのみになります。

今後のgen02サイジングガイダンスの削除

Black Duck 2023.10.0では、gen02のサイジング ガイダンスおよびドキュメントが削除されます。サイジングのリファレンスについては、「[Black Duckハードウェアのスケールリング ガイドライン](#)」ページを参照してください。

今後のPostgreSQL 13のサポートの終了

今後の2023.10.0リリースで、Black Duckは外部PostgreSQL 13のサポートを終了します。詳しくは、「[PostgreSQL Version Upgrade Schedule](#)」ページを参照してください。

今後のPostgreSQLコンテナのバージョン14への移行

Black Duck は、2023.10.0リリースでPostgreSQLイメージをバージョン14に移行します。Black DuckのPostgreSQLイメージを使用していないお客様には影響はありません。

今後のPostgreSQLコンテナユーザーに対するアップグレードの制限

2023.10.0以降、Black Duckでは、PostgreSQL 11またはPostgreSQL 13コンテナを使用するBlack Duckバージョンからの直接アップグレードのみがサポートされるようになります(具体的には、2022.2.0から2023.7.x(両端を含む)までのすべてのBlack Duckバージョン)。古いBlack Duckバージョン(具体的には、2022.2.0より前のすべてのBlack Duckバージョン)からアップグレードするBlack Duck提供のPGコンテナのユーザーは、2023.7.xにアップグレードしてから、2023.10.xにアップグレードするという、2段階アップグレードを行う必要があります。

ドキュメントのローカライゼーション

UI、オンラインヘルプ、およびリリースノートのバージョン2023.4.0が日本語と簡体字中国語にローカライズされました。

新機能および変更された機能

PostgreSQL 15の外部データベースのサポート

Black Duck は、外部PostgreSQLを使用する新規インストール用にPostgreSQL 15をサポート・推奨するようになりました。PostgreSQL 15は、Azure Database for PostgreSQLではまだサポートされていないため、Black Duckでは、この環境をご利用のユーザーにはPostgreSQL 14フレキシブル サーバーの使用を推奨しています。

Black Duck 2023.7.xへの移行では、PostgreSQL 15への移行は不要です。

内部PostgreSQLコンテナのユーザーは、アクションは必要ありません。

レポートオブジェクトタイプの暗号化

Black Duck 2023.7.0では、オブジェクト ストアに格納されているレポート オブジェクトが、保存されているFILEボリュームで保存時の暗号化の対象となるように、それらのレポート オブジェクトを機密とマークするようになりました。それらを暗号化するためには、適切なシークレットが提供されている環境でBlack Duck Cryptoを有効にする必要があります。ご利用の環境のBlack Duck Crypto設定に応じて、次の動作の変更が適用されます。

2023.7.0へのアップグレード時にBlack Duck Cryptoが有効化されていない環境の場合

すべての既存レポートおよびすべての新規レポートはディスク上で暗号化されないままですが、機密としてマークされます。その後、Black Duck Cryptoが有効化された場合は、これらのオブジェクトはその機密特性に準拠するため、バックグラウンドで暗号化されます。

2023.7.0へのアップグレード時にBlack Duck Cryptoがすでに有効化されている環境の場合

Black Duck Cryptoをすでに有効化している場合は、既存のレポートは暗号化されないままになり、新規レポートはすべて暗号化されます。すべてを強制的に暗号化する必要がある場合は、環境変数SYNOPSISYS_CRYPTOROTATE_RESOURCES_ON_STARTUP=trueを設定します。これにより強制的に、システムで内部キーがローテーションされ、暗号化されていない古いレポートを含むすべてのレポートが再暗号化されます。

ストレージサービスオブジェクトの暗号化

Black Duck Cryptoが有効化されている場合は、オブジェクト ストレージのFILEボリュームに格納されている機密オブジェクトが保存時に暗号化されます。

[ジョブ]ページの更新

[ジョブ]ページは、表示される情報の使いやすさと拡張性を向上させるために再設計されました。[ジョブ]ページは、次の3つのタブで構成されています。

- ・ 完了: 成功または失敗にかかわらず、完了したすべてのジョブが表示されます。
- ・ スケジュール済み: ご使用の環境で実行するようにスケジュールされているすべてのジョブが表示されます。
- ・ 処理中: 現在進行中のすべてのジョブが表示されます。

新しい[マッチしない取得元]管理ページ

Black Duckがパッケージ スキャン中に特定したが、コンポーネント バージョンにマップできなかった取得元IDの管理が容易になりました。[マッチしない取得元]ページで、カスタムコンポーネントにマッピングを追加または削除できます。マッピングは、後続のパッケージマネージャスキャンに追加されます。[マッチしない取得元]ページにアクセスするには、[管理]>[マッチしない取得元]をクリックします。

さらに、[コンポーネントバージョン]ページでカスタムコンポーネントにマッピングされる取得元IDも管理できるようになりました。

カスタムコンポーネントとのマッチングにはDetect 7以降を使用する必要がありますが、現在はパッケージマネージャスキャンでのみサポートされています。

通知ファイルレポートの強化

通知ファイルレポートに、次の新しいオプションを追加できるようになりました。

- ・ ディープライセンスデータ: コンポーネントの取得元によって検出されるディープライセンス。プロジェクトでディープライセンスが有効な場合にのみ使用できます。
- ・ ファイル著作権テキスト: ファイルマッチで検出された著作権テキスト。ファイルマッチが存在する場合にのみ使用できます。
- ・ マッチしないファイル検出: プロジェクト内のコンポーネントに関連付けられていないファイル検出。プロジェクトにマッチしないファイルが存在する場合にのみ使用できます。
- ・ ファイルライセンスデータ: ファイルマッチで検出されたライセンス。ファイルマッチが存在する場合にのみ使用できます。

新しいSBOMレポートフィールド

SBOMレポートのSPDXバージョンに、次の2つの新しいオプションフィールドが含まれるようになりました。

- ・ パッケージコメント: 記述されているパッケージに関する全般的なコメント。
- ・ パッケージ有効期限日: サプライヤから取得したパッケージのサポート期間の終了日。

最初に、[管理]>[SBOM]>[構成表コンポーネント]でこれらのフィールドをアクティブ化する必要があります。有効化されたら、プロジェクトバージョンの構成表に移動し、コンポーネントの行の端にある[オプション]ボタンをクリックしてから、SBOMフィールドを選択することで、フィールドを更新できます。

構成表フィルタラベルの更新

[構成表プロジェクトバージョン]ページの[コンポーネント]タブの[マッチステータス]フィルタには、あいまいな名前が付けられていました。このフィルタはスニペットマッチにのみ適用されるため、この具体的なユースケースを正しく表すために、名前が[スニペットマッチステータス]に変更されました。

ロギング情報の強化

成功したログインと失敗したログインの両方について、ユーザーがユーザー名とパスワードを使用してログインしたときのロギング情報(認証コンテナ)が追加されました。

削除されたプロジェクトを含むレポートへのアクセス権限の更新

レポートへのアクセス権限が更新され、いずれかのプロジェクトが削除された場合には、レポートの(削除されていない)残りのプロジェクトすべてに対するアクセス権限を持っているか、ユーザー役割にグローバルなプロジェクト読み取りアクセスが含まれているユーザーがレポートにアクセスできるようになりました。そのいずれにも当てはまらないユーザーは、レポートにアクセスできません。

バージョンの詳細レポートの強化

バージョンの詳細レポートに、サブプロジェクトの更新が含まれるようになりました。

- ・ バージョンの詳細の更新ガイダンスレポートに、サブプロジェクトのアップグレードガイダンスが含まれるようになりました。
- ・ プロジェクトバージョン更新ガイダンスレポートの最初の列が[使用者]になりました。これは、空白でない場合、アップグレードガイダンスのサブプロジェクトを報告します。

レポート生成の強化

レポートデータの収集とレポート形式での作成のメカニズムが、メモリ使用量を抑制するように改善されました。この変更の結果として、レポートの生成にかかる時間が長くなる可能性があることに注意してください。

KnowledgeBase環境変数の統合

Black Duck には、さまざまなKnowledgeBaseサービスのKnowledgeBaseスキーム、ホスト、ポート構成を制御するためのさまざまな環境変数が用意されています。Black Duck 2023.7.0以降、構成を簡素化するために、次の変数に対するKnowledgeBase環境変数構成が統合されました。

- ・ BLACKDUCK_KB_SCHEME
- ・ BLACKDUCK_KB_HOST
- ・ BLACKDUCK_KB_PORT

次のプロパティプレフィックスは明示的に削除され、参照されなくなります。

- ・ BLACKDUCK_KBCLOUD
- ・ BLACKDUCK_KBDETAIL
- ・ BLACKDUCK_JSONWEBTOKEN

カスタマイズのために古いKnowledgeBase環境変数を手動で上書きしたユーザーは、環境が機能していることを確認する必要があります。

UIの日付選択ツールの更新

UIで使用される日付選択ツールが更新され、機能と、(ブラウザによっては)外観が変更されます。これは、ブラウザの言語でローカライズされるわけではないことに注意してください(Firefoxを除く)。Chrome、Edge、Safariでは、オペレーティングシステムのロケールに従うようになります。

サポートされるブラウザのバージョン

- ・ Safariバージョン16.4
 - ・ Safariバージョン14以前はサポートされなくなりました

2. Previous Releases · Black Duck 2023.7.x

- ・ Chromeバージョン114.0.5735.198(公式ビルド)(x86_64)
 - ・ Chromeバージョン91以前はサポートされなくなりました
- ・ Firefoxバージョン114.0.2(64ビット)
 - ・ Firefoxバージョン89以前はサポートされなくなりました
- ・ Microsoft Edgeバージョン114.0.1823.67(公式ビルド)(64ビット)
 - ・ Microsoft Edgeバージョン91以前はサポートされなくなりました

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:13-2.27
- ・ blackducksoftware/blackduck-authentication:2023.7.0
- ・ blackducksoftware/blackduck-webapp:2023.7.0
- ・ blackducksoftware/blackduck-scan:2023.7.0
- ・ blackducksoftware/blackduck-jobrunner:2023.7.0
- ・ blackducksoftware/blackduck-cfssl:1.0.20
- ・ blackducksoftware/blackduck-logstash:1.0.32
- ・ blackducksoftware/blackduck-registration:2023.7.0
- ・ blackducksoftware/blackduck-nginx:2.0.47
- ・ blackducksoftware/blackduck-documentation:2023.7.0
- ・ blackducksoftware/blackduck-upload-cache:1.0.45
- ・ blackducksoftware/blackduck-redis:2023.7.0
- ・ blackducksoftware/blackduck-bomengine:2023.7.0
- ・ blackducksoftware/blackduck-matchengine:2023.7.0
- ・ blackducksoftware/blackduck-webui:2023.7.0
- ・ blackducksoftware/blackduck-storage:2023.7.0
- ・ sigsynopsys/bdba-worker:2023.6.0
- ・ blackducksoftware/rabbitmq:1.2.28

APIの機能強化

PUT /api/settings/data-retentionの削除

2023.4.0リリースノートに記載されているとおり、PUT /api/settings/data-retentionはPATCH /api/settings/data-retentionのために非推奨になり、呼び出された場合はHTTP 405 METHOD_NOT_ALLOWEDエラーメッセージが返されます。これは、Black Duck 2023.7.0では完全に削除されており、使用された場合はHTTP 404 NOT_FOUNDエラーメッセージが返されるようになります。

GET api/external-config/detect-uriの非推奨

GET api/external-config/detect-uri APIリクエストは非推奨になり、GET api/settings/detectに置き換えられました。非推奨にはなりませんが、ユーザーは引き続き古いAPIを使用できます。

GET `api/external-config/detect-uri`は非推奨になりましたが、役割を持たない認証ユーザーは引き続き、これを使用してAPI文字列を取得できます。これらのユーザーがGET `api/settings/detect` APIを使用した場合は、`detectUri` (設定されている場合)のみを受け取ります。

PUT `/api/policy-rules/{policyRuleId}`のパフォーマンスの向上

プロジェクトバージョンのコンポーネントを評価した後で、違反の変更が検出された場合にのみ、ポリシープロファイルの計算が実行されるように制限することで、PUT `/api/policy-rules/{policyRuleId}` APIリクエストのパフォーマンスが改善されました。

POST `api/components/{componentId}/versions`の更新

新規カスタムコンポーネントバージョンの作成時に、ユーザーが外部IDをこのバージョンにマップできるように、POST `api/components/{componentId}/versions` APIリクエストが更新されました。

新しいパブリックSBOMフィールドエンドポイント

PUT `/api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/sbom-fields` エンドポイントで、構成表コンポーネントのSBOMフィールドの保存された値が更新されました。

バイナリスキャナ情報

バイナリスキャナがバージョン2023.6.0に更新されました。

- `package-lock.json`ファイルのスキャンがサポートされるようになったため、以前のスキャンでは検出されなかった、追加のコンポーネントが示される場合があります。その結果、検出されるコンポーネント数が増大する可能性があります。

修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-21449)。違反が軽減された場合に、ネスト化されたコンポーネントの脆弱性の数について誤ったポリシー違反が表示されるという問題を修正しました。
- (HUB-33362)。XMLファイルを使用してSAMLを設定しようとしたときに、SAMLが無効化されていないとファイルが保存されないという問題を修正しました。
- (HUB-34720)。ライセンスIDは変更せずに、汎用ライセンステキストの代わりに元のテキストを反映するなどのためにライセンスを変更した場合に、変更がSPDXファイルにエクスポートされない問題を修正しました。
- (HUB-35512)。同じコンポーネント+バージョン+取得元を使用して、[構成表]ページに手動でコンポーネントバージョンを追加した場合に、元の設定が削除されていても、[既に存在するため、構成表コンポーネントを手動で追加できません。]というエラーメッセージが表示され続けるという問題を修正しました。
- (HUB-37067)。[検索]>[脆弱性]ページから、修正ステータスフィルタが削除されました。
- (HUB-37626)。v1.3またはv1.4いずれかのJSON形式のSBOMレポートを、UIで、またはAPIを介して生成し、`/api/projects/{projectId}/versions/{projectVersionId}/reports/{reportId}/contents`によってそのレポートを取得しようとすると、「`/n`」文字を含む非JSON形式でレポートが表示される問題を修正しました。
- (HUB-37763)。ライセンス管理のコンポーネント数APIが、リンクされている「使用場所」の数の結果と一致しないという問題を修正しました。
- (HUB-37796)。MaaSで、[コードの場所を作成または更新できませんでした]というエラーでスキャンが失敗することがある問題を修正しました。
- (HUB-37922)。100を超えるコンポーネントを指定して、構成表で一括操作機能を使用しようとした場合の問題を修正しました。

- ・ (HUB-38146)。プロジェクトバージョン名にフォワードスラッシュ文字(/)が含まれている場合に、レポートの生成でサブフォルダが作成される問題を修正しました。フォワードスラッシュ文字は、下線文字(_)で置き換えられるようになります。
- ・ (HUB-38347)。DockerイメージInspectorスキャンの実行時に、署名スキャンツールの問題によってソースコードのサイズが正しく計算されず、その結果スキャンが失敗することがあるという問題を修正しました。
- ・ (HUB-38480)。使用している並べ替えオプションにかかわらず、APIリクエスト/api/projectsが常に名前ですべて置換えられるという問題を修正しました。
- ・ (HUB-38535)。ライセンス承認ステータスが変更された後で、/api/components/<component ID>/versions/<version ID>/licenses/<license ID> APIリクエストが正しいライセンス承認ステータスを返さないという問題を修正しました。
- ・ (HUB-38554)。HUB UIを使用してKBコンポーネントバージョンを移動するときに、ユーザーが指定した内容にかかわらず、ページネーションが強制的に25に設定されるという問題を修正しました。
- ・ (HUB-38587)。kbMatchTimeoutPropertyは常にblackduck-config.envファイルから読み取る必要があるにもかかわらず、この値が誤ってハードコーディングされた値(100,000ms)に設定されるという問題を修正しました。
- ・ (HUB-38590)。[コンポーネントの追加]ダイアログボックスの[すべての取得元]ドロップダウンに10行しか表示されないために、一部の取得元が表示されない場合があるという問題を修正しました。
- ・ (HUB-38598)。コンポーネントマネージャの役割が、カスタムコンポーネントバージョンの作成後にこのバージョンにアクセスしようとすると、403 Forbiddenエラーが表示される場合があるという問題を修正しました。
- ・ (HUB-38646)。SCM統合を使用すると、プライベートリポジトリが表示されない問題を修正しました。変更を有効にするには、Black Duckから既存のトークンを削除する必要がある場合があることに注意してください。
- ・ (HUB-38679)。コンポーネントレポートの[要履行]列には、コンポーネントバージョンの「承認済みステータス」が含まれているため、利便性を向上させるために列の名前を[コンポーネントバージョンステータス]に変更しました。
- ・ (HUB-38685)。設定の更新後に、プロジェクトの自動削除で新しい設定が使用されないという問題を修正しました。
- ・ (HUB-38720)。ライセンステキストエリアが小さすぎるという問題を修正しました。
- ・ (HUB-38774)。プロジェクトバージョン内で[リリース日]フィールドの設定を解除しようとしても反映されず、以前に設定された日付が残されるという問題を修正しました。

Black Duck 2023.4.x

Black Duck バージョン2023.4.2

- ・ [発表](#)
- ・ [新機能および変更された機能](#)
 - ・ [APIの機能強化](#)
 - ・ [バイナリスキャナ情報](#)
 - ・ [修正された問題](#)

発表

Black Duck 2023.4.2に関する新たな発表はありません。

新機能および変更された機能

Black Duck 2023.4.2には、新機能や変更された機能はありません。

APIの機能強化

Black Duck 2023.4.2には、新規のまたは変更されたAPIリクエストはありません。APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

バイナリスキャナ情報

Black Duck 2023.4.2のバイナリ スキャナに関する変更はありません。

修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (HUB-25500)。AWSで実行しているユーザーが、この問題の回避策を有効にするためのメカニズムを追加しました。この問題が発生しているユーザーは、upload-cacheサービスからCPU使用率が高いことが示された場合、Black Duckサポートに連絡することをお勧めします。この問題は、次回のBlack Duck 2023.10.0リリースで修正される予定です。
- ・ (HUB-38587)。kbMatchTimeoutPropertyが誤ってハードコーディングされた値(100,000ms)に設定される問題を修正しました。この値は、想定どおりにblackduck-config.envファイルから読み取られるようになります。
- ・ (HUB-38735)。PostgreSQL 9.6またはPostgreSQL 11ベースのBlack DuckバージョンからBlack Duck 2023.4.1にアップグレードする場合に、PostgreSQLコンテナを使用していると、postgres-upgraderが失敗し、アプリケーションが起動しないことがある問題を修正しました。
- ・ (HUB-38815)。スキャンが失敗する原因となる可能性がある、Black Duck高速スキャンでの断続的なResourceAccessExceptionエラーを修正しました。

Black Duck バージョン2023.4.1

- ・ [発表](#)
- ・ [新機能および変更された機能](#)
 - ・ [APIの機能強化](#)
 - ・ [バイナリスキャナ情報](#)
 - ・ [修正された問題](#)

発表

ストレージおよび登録に対するノード制約

Black Duck 2023.4.1では、複数ノードのswarm導入を使用しているユーザーは、ストレージと登録に対するノード制約をチェックするように求められます。この変更によって、複数システム間でのコンテナによるノードの移動やデータの分散が軽減されます。

```
#deploy:
#  placement:
#    constraints:
#      - node.labels.type == db
```

新機能および変更された機能

マッチしないファイルデータのパーズの改善

アーカイブ済みプロジェクトフェーズのプロジェクトバージョンについてのみ、マッチしないファイルデータをパーズできるようにしました。これをグローバルに実行するには、[管理者]>[システム設定]>[データ保持]ページを使用します。これはすべてのプロジェクトに反映されます。または、[設定]ページで選択したプロジェクトに対し、ローカルに実行できます。

グローバル設定は、独自の設定を明示的に指定していないプロジェクトおよびスキャンにのみ適用されます。同様に、グローバル設定の変更は、独自の設定を指定しているプロジェクトまたはスキャンには影響しません。

ポリシーに対するSBOMレポートの検証

ポリシーに照らしてSBOMレポートの生成を検証するように、特定のプロジェクトグループを構成できるようになりました。

(プロジェクトグループへのアクセス権がある場合に)プロジェクトグループレベルで新しい設定を有効にすると、ポリシー違反のあるプロジェクトでSBOMレポートが生成されないようにすることができます。また、グループ内のプロジェクトまたはすべての子グループ内のすべてのプロジェクトに設定を適用することもできます。

この設定が有効な場合に、SBOMレポートを生成しようとする、プロジェクトにポリシー違反があるためにレポートを生成できないことが通知されます。

SBOMレポートの新しいSPDX v2.3サポート

プロジェクトのソフトウェア構成表レポートをSPDX v2.3形式でエクスポートできるようになりました。

新しいプロジェクトエイリアスSBOMフィールド

プロジェクトレベルでプロジェクト名およびバージョン情報フィールドを上書きするための、新しいオプションのプロジェクトエイリアスSBOMフィールドが追加されました。最初に、[管理]>[SBOM]>[プロジェクト]でフィールドをアクティブ化する必要があります。有効化したら、プロジェクトのページ>[設定]でプロジェクトのエイリアスを変更できます。

APIの機能強化

更新されたスキャンエンドポイントのBDIOヘッダー情報

次のAPIエンドポイントは、HTTPヘッダーではなく、BDIOヘッダーのプロジェクトおよびバージョン名を使用するように更新されました。

- /api/scan/data
- /api/intelligent-persistence-scans
- /api/intelligent-persistence-scans/{scanId}
- /api/developer-scans
- /api/developer-scans/{scanId}

バイナリスキャナ情報

修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-33736)。いくつかのAPIエンドポイントが、HTTPヘッダーではなく、BDIOヘッダーのプロジェクトおよびバージョン名を使用するように更新されました。詳しくは、「APIの機能強化」セクションを参照してください。

- ・ (HUB-36776)。[ソース]タブのコンポーネントに対して[ファイルツリーで表示]を選択した場合に、バイナリスキンのファイル部分で、左側のファイルツリーにファイルが表示されない問題を修正しました。
- ・ (HUB-37280)。SPDX 2.2で、「filesAnalyzed」がfalseに設定されているのに、すべてのプロジェクトファイルが一覧表示される問題を修正しました。
- ・ (HUB-38005)。サポートされなくなったため、[脆弱性報告済み]並べ替えオプションが、[検索]>[コンポーネント]ページから削除されました。
- ・ (HUB-38141)。スキャンクライアントが、マッチするいずれのディレクトリまたはアーカイブにも属しておらず、まだデータベースに保存されていないソースファイルを要求したときに、スニペットスキャン結果の一貫性が失われる可能性がある競合状態を修正しました。
- ・ (HUB-38212)。CycloneDXレポートをインポートするときに、Nullポインタ例外エラーが発生する可能性がある問題を修正しました。
- ・ (HUB-38244)。プロキシの背後で実行しているときにSIG Artifactoryと通信すると、[構成の検出]ページにエラーメッセージが表示されることがある問題を修正しました。
- ・ (HUB-38279)。Black Duck UIの[ダッシュボード]タブで、[現在のビューをエクスポート]ボタンを使用した場合に[保存済み検索]の現在のビューがエクスポートされない問題を修正しました。
- ・ (HUB-38312)。サブプロジェクト内の一括で無視されたコンポーネントの脆弱性の変更が、親プロジェクトに反映されない問題を修正しました。
- ・ (HUB-38328)。正しくないi18n文字が原因で、日本語設定でポリシー上書き日付情報が正しく表示されないという問題を修正しました。

Black Duck バージョン2023.4.0

- ・ [発表](#)
- ・ [新機能および変更された機能](#)
 - ・ [APIの機能強化](#)
 - ・ [バイナリスキナ情報](#)
 - ・ [修正された問題](#)

発表

Azure PostgreSQLユーザー向けの2023.4.0へのアップグレード

Azure PostgreSQLを使用してアップグレードまたはインストールする場合、データベース管理者は、2023.4.0以降をインストールまたはこれ以降にアップグレードする前に、hstore PostgreSQL拡張機能のインストールを有効にする必要があります。

pgcrypto拡張機能をstスキーマに移動

Black Duck 2023.4.0以降、pgcrypto PostgreSQL拡張機能は、パブリック スキーマからstスキーマに移動されます。外部PostgreSQLインスタンスを使用してアップグレードしており、なおかつ、blackduckデータベースユーザーがスーパーユーザーではない場合、次のコマンドを使用して拡張機能を手動で再配置する必要があります。

```
alter extension pgcrypto set schema st ;
```

それ以外の場合は、移動は自動的に実行されます。

jobrunnerではMAX_CONCURRENT_JOBSを使用対象から削除

MAX_CONCURRENT_JOBSは、Black Duck 2022.10.xで廃止となり、このリリースで削除されました。新しいメカニズムの設定については、SwarmとKubernetesのインストールガイドを参照してください。

MaaS対応システムでのKBMATCH_SENDFPATHの廃止

Black Duck 2023.4.0では、Match as a Service (MaaS、サービスとしてのマッチング) が一般的に利用できるようになりました。新規のお客様の場合は、デフォルトで有効になり、既存のすべてのお客様の場合は、標準で利用できるようになっています。このアップデートの結果、KBMATCH_SENDFPATH (マッチングのためにナレッジベースにファイルパス メタデータを送信する機能を無効にするオプション) は、Black Duckの今後のリリースで削除されることになりました。

このオプションを引き続き使用する場合は、Black Duckサポートに連絡して、Black Duck登録キーに対応しているMaaSを無効にもらう必要があります。

今後のDocker 18.09.xおよび19.03.xのサポート終了

2023.7.0リリース以降、Black DuckはDocker 18.09.xおよび19.03.xをサポートしなくなります。サポートされるバージョンはDocker 20.10.xのみになります。

Black Duckctl利用期間の終了予定

2023.7.0リリース以降、Black Duckctlはサポートされなくなり、更新も行われなくなります。Black Duckctlのドキュメントは、<https://github.com/blackducksoftware/hub/tree/master/kubernetes/blackduck>にあります。

今後のコンテナスキャンのハードウェア要件

Black Duck 2023.10.0では、コンテナ スキャンの実行にBDBAコンテナが必要になります。つまり、現在Black Duckでコンテナ スキャンを実行していて、Black DuckインスタンスにBDBAを導入していないお客様は、新しいコンテナ スキャン機能を利用するために、2023.10.0リリースのガイダンスに従い、追加のハードウェア リソースを割り当てる必要があります。

この変更の一環として、コンテナスキャンの既存の機能が削除されることはありません。

ドキュメントのローカライゼーション

UI、オンラインヘルプ、およびリリースノートのバージョン2023.1.0が日本語と簡体字中国語にローカライズされました。

新機能および変更された機能

新しいSBOMアップロード機能

Black Duckの[スキャン]ページが更新され、レポート アップロード時の対象ファイル タイプが仕分けされました。[ファイルのアップロード]ボタンをクリックすると、[BDIOスキャン]、[SBOM-SPDX]、[SBOM-CycloneDX]のいずれかを選択できます。

新しい構成表マッチスコア機能

署名スキャンの実行時には、マッチ対象にあいまいさが生じることがあります。特定のコンポーネントとバージョンでマッチを評価できますが、他の複数のコンポーネントとバージョンがマッチする可能性もあります。

2023.4.0の新機能として、プロジェクトバージョンの構成表では、新しい列にコンポーネントのマッチスコアが表示されます。マッチしたコンポーネントは、マッチスコアが高いほど、期待している実際のコンポーネントおよびバージョンである確実性が高くなります。

マッチスコアのしきい値の計算方法は、[管理者] > [システム設定] > [コンポーネントマッチスコア]で設定できます。マッチスコアのしきい値を設定することで、あいまいなマッチと低いパーセンテージのマッチを減らすことができ、マッチ結果に表示される誤検出を減らすことができます。しきい値の設定が高すぎると、マッチ結果から正しい検出を失う可能性があることに注意してください。

新しいマッチあいまいさロジックでシステムが改善された結果、構成表の表示時に、異なる結果が表示されることがあります。

Black Duck Detectの新しいホスティング/バージョン集中管理

Black Duck は、ニーズに応じてBlack Duck Detectに接続できるように、Black Duckホスト型という新しい接続方法を提供しています。この方法は、自主管理を望まず、使用するDetectのバージョン管理をBlack Duckに委任したいお客様に最適です。Black Duckのシステム設定では、Detectのメジャー バージョンと最新の正確なバージョンがドロップダウン リストに表示されます。このリストでは、スキャンの実行対象を選択できます。

Artifactory Integrationの新機能

Black Duck 2023.4.0では、JFrog Artifactoryを使用しているKubernetesユーザーが、アーティファクトを対象として、バイナリ スキャンとDockerイメージ/コンテナ スキャンの両方を実行できるようになりました。また、以前のフェーズでサポートされていた署名スキャンが拡張されました。現在、完全なオンプレミスとハイブリッドという2つの導入オプションがサポートされています。導入の要件と手順については、Kubernetesのインストールガイドを参照してください。

全スキャンインGRESSエンドポイントでの新しいスキャンレート制限

ヒープメモリを基準としている環境で、使用可能な割り当てヒープの80%(HUB_MAX_MEMORY)超がスキャンコンテナで使用されている場合、ヒープ使用率が60%に下がるまで待ってから、スキャンが再実行されることになります。またコンテナでは、レート制限が有効でアクティブになっている場合でも、300秒(blackduck.scan.ingress.scanPassThroughIntervalSecsのデフォルト値)に1回はスキャンを実行できます。

新しいBlack Duckストレージコンテナ

Black Duck 2023.1.0では、新しいストレージ サービスが導入されました。このサービスでは、静的ファイル(SBOMやその他のレポートなど)を永続ストレージに移動できます。このサービスにより、データベースの領域が解放され、スキャン パフォーマンスとスケーラビリティの強化が可能になっています。

注:Black Duck 2023.1.0リリース ノートでは、この項目が誤って抜け落ちていました。

Blackduck Storageの新しいカスタムボリュームの構成

2023.4.0以降、ストレージコンテナは、ファイルベースのオブジェクトを保存するために、最大3個のボリュームを使用するように構成できます。さらにこの構成は、あるボリュームから別のボリュームにオブジェクトを移行するように設定できます。バックアップスクリプトhub_create_data_dump.shおよびhub_db_migrate.shが更新され、それに応じて、ファイルプロバイダボリュームが保存されました。

ヒートマップ用の新しいフィルタリングサポート

ヒートマップの表示データをフィルタリングできるようになりました。フィルタリングオプションには、コードの場所ID、コードの場所名、プロジェクト名、スキャンデータ、スキャンステータス、スキャンタイプ、バージョン名が含まれます。

構成表サポートのための拡張高速スキャン結果データ

構成表のサポートのために、高速スキャンを設定して、データポイントを含めた完全な結果形式を提供できるようになりました。これを実行するには、次の環境変数を設定します。BLACKDUCK_RAPID_SCAN_EXTENDED_DATA=true.新しいデータポイントには、次のものが含まれます。

・ componentDescription	・ リリース日	・ SPDXライセンスID
・ ホームページへのリンク	・ コンポーネントID、コンポーネン	・ ソース(NVDまたはBDSDA)
・ OpenHubリンク	トバージョンID、コンポーネン	・ マッチタイプ
・ 宣言されたライセンス定義	バージョン取得元URIへのメタリ	
	ンク	

- ・ 外部名前空間
- ・ パッケージURL

ポリシー違反管理の強化

Black Duck構成表ページで、ポリシー上書きの有効期限(日付)を設定できるようになりました。コンポーネントの違反アイコンをクリックすると、ポリシー違反の上書き状態を続ける期間の最終日を入力できます。この有効期限が切れると、違反状態に戻ります。

依存関係ツリービューの強化

依存関係ツリービューでは、必要な情報を強調表示してコピー/ペーストできるようになりました。

Detect DesktopのCentOSダウンロードリンクの削除

[ツール]ページが更新され、Detect DesktopのCentOSダウンロードリンクが削除されました。これは、Black Duckではサポートされていないためです。

PostgreSQL 15の予備的なサポート

Black Duck 2023.4.0では、外部データベースとしてPostgreSQL 15を使用できるように、事前サポートが追加されました。このサポートはテスト専用です。本番環境での使用はサポートされていません。

サポートされるブラウザのバージョン

- ・ Safariバージョン16.3(17614.3.7.1.7、17614)
 - ・ Safariバージョン13.1以前はサポートされなくなりました
- ・ Chromeバージョン111.0.5563.146(公式ビルド)(x86_64)
 - ・ Chromeバージョン79以前はサポートされなくなりました
- ・ Firefoxバージョン111.0.1(64ビット)
 - ・ Firefoxバージョン74以前はサポートされなくなりました
- ・ Microsoft Edgeバージョン111.0.1661.62(公式ビルド)(64ビット)
 - ・ Microsoft Edgeバージョン79以前はサポートされなくなりました

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:13-2.22
- ・ blackducksoftware/blackduck-authentication:2023.4.0
- ・ blackducksoftware/blackduck-webapp:2023.4.0
- ・ blackducksoftware/blackduck-scan:2023.4.0
- ・ blackducksoftware/blackduck-jobrunner:2023.4.0
- ・ blackducksoftware/blackduck-cfssl:1.0.17
- ・ blackducksoftware/blackduck-logstash:1.0.29
- ・ blackducksoftware/blackduck-registration:2023.4.0
- ・ blackducksoftware/blackduck-nginx:2.0.38
- ・ blackducksoftware/blackduck-documentation:2023.4.0

- blackducksoftware/blackduck-upload-cache:1.0.40
- blackducksoftware/blackduck-redis:2023.4.0
- blackducksoftware/blackduck-bomengine:2023.4.0
- blackducksoftware/blackduck-matchengine:2023.4.0
- blackducksoftware/blackduck-webui:2023.4.0
- blackducksoftware/blackduck-storage:2023.4.0
- sigsynopsys/bdba-worker:2023.3.0
- blackducksoftware/rabbitmq:1.2.21

APIの機能強化

コンポーネントエンドポイントの更新

次のパブリックAPIエンドポイントが更新され、コンポーネント、バージョン、取得元IDを更新できるようになりました。

- PUT /api/projects/{projectId}/versions/{projectVersionId}/components
- PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}

新しいJobHistoryAppService APIエンドポイント

2つの新しいパブリックREST APIエンドポイントが追加されました。これらは、JobRuntimeRepositoryを使用して、ジョブランタイムに関する情報を取得し、これらの情報を提供します。

- /api/jobs-histories
- /api/jobs-histories-filters

新しいJobRuntimeAppService APIエンドポイント

2つの新しいパブリックREST APIエンドポイントが追加されました。これらは、JobRuntimeRepositoryを使用して、ジョブランタイムに関する情報を取得し、これらの情報を提供します。

- /api/jobs-runtimes
- /api/jobs-runtimes-filters

実行中のジョブを表示するには、/api/job-runtimesエンドポイントを使用する必要があります。ご注意ください。新しいエンドポイントのために、既存の/api/jobsエンドポイントは廃止されます。

新しいJobScheduleAppService APIエンドポイント

3つの新しいパブリックREST APIエンドポイントが追加されました。これらは、システムでスケジュールされているジョブのリストを出力します。

- /api/jobs-schedules
- /api/jobs/schedulers/{scheduler}/trigger-groups/{triggerGroup}/triggers/{triggerId}
- /api/jobs-schedules-filters

スケジュールされたジョブを表示するには、/api/job-schedulesエンドポイントを使用する必要があります。ご注意ください。新しいエンドポイントのために、既存の/api/jobsエンドポイントは廃止されます。

新しいJobRunner APIエンドポイント

新しいパブリックREST APIエンドポイントが追加されました。このエンドポイントでは、定期的なジョブを有効または無効にできます。このように設定を変更すると、システムで予期しない動作が発生する可能性があります。ご注意ください。

- ・ `/api/jobs-schedules-configurations`

Detectの新しい集中バージョン管理APIエンドポイント

Black Duck 2023.4.0で提供されるDetectの新しい集中バージョン管理機能をサポートするために、次のエンドポイントが追加されました。

- ・ `GET /api/settings/detect`
 - ・ 現在のDetectバージョン管理設定を取得します
 - ・ システム管理者ではない認証ユーザーがアクセスした場合、これらのユーザーはdetectUri値のみを受信します(値がある場合)。
 - ・ 認証されたシステム管理者がアクセスした場合、管理者は次の情報を受信します。
 - ・ `detectUri`: システム管理者が保存したDetect URI。
 - ・ `useInternalHosting`: ブール値。Detectに使用するホスティング タイプ(内部ホスト型またはBlack Duckホスト型)を判断します。内部ホスト型のDetectバージョンを使用していない場合はfalseを返します。
 - ・ `useMajorVersion`: ブール値。最新メジャーバージョンのDetectが使用されているかどうかを判定します。UIで[最新8.x]または[最新7.x]が選択されている場合はtrueを返します。
 - ・ `selectedVersion`: 文字列。使用されているDetectのバージョンを返します。
 - ・ `allowDowngrade`: ブール値。システム設定で、ユーザーが古いバージョンのDetectを使用できるかどうかを通知します。
 - ・ `majorVersions`: 文字列。Detectの現在有効なメジャーバージョンのリスト。
 - ・ `allVersions`: 文字列。Detectの現在有効な全バージョンのリスト。
- ・ `PATCH /api/settings/detect`
 - ・ Detectのバージョン管理設定を更新します
 - ・ システム管理者ユーザーによる認証アクセスが必要です
 - ・ 次の情報を更新します。
 - ・ `detectUri`: Detectの内部URI。
 - ・ `useInternalHosting`: ブール値。Detectに使用するホスティング タイプ(内部ホスト型またはBlack Duckホスト型)を設定します。
 - ・ `useMajorVersion`: ブール値。Detectの最新メジャーバージョンまたは明示的バージョンを設定します。useInternalHostingがfalseの場合は更新されます。これは必須です。
 - ・ `selectedVersion`: 文字列。使用するDetectバージョン。メジャーバージョンまたは正確なバージョンのどちらかです。useInternalHostingがfalseの場合にのみ更新されます。
 - ・ `allowDowngrade`: Boolean。管理されている場合、以前のバージョンのDetectを使用できます。

PUT /api/settings/data-retentionの廃止

2022.10.0リリースノートに記載されているように、PUT /api/settings/data-retentionは廃止され、PATCH /api/settings/data-retentionに置き換えられました。Black Duck 2023.4.0では、PUT /api/settings/data-retentionは、HTTP 405 METHOD_NOT_ALLOWEDエラー メッセージを返すようになりました。

バイナリスキャナ情報

バイナリスキャナがバージョン2023.3.0に更新されました。

。

修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (HUB-32471)。スキャン時にKnowledgeBaseに接続できなかった場合、状況がUIで報告されず、構成表が空になっていました。この問題を修正しました。
- ・ (HUB-33018)。構成表を印刷するときに、縦方向および横方向のスクロールバーが表示されていました。この問題を修正しました。
- ・ (HUB-34474)。プロジェクト名に全角大文字が含まれている場合に、フィルタリングしたプロジェクトが正しく表示されませんでした。この問題を修正しました。
- ・ (HUB-34616)。[診断]ページにジョブが表示された場合に、完了ジョブのミリ秒が表示されませんでした。この問題を修正しました。
- ・ (HUB-34964)。検索ページに表示される脆弱性の[使用者]数は、脆弱性の影響を受けるプロジェクトのページに表示される値と一致していませんでした。この問題を修正しました。
- ・ (HUB-34981)。コンポーネント バージョン リスト ビューの[使用者]数がコンポーネント バージョン詳細ビューの値と一致していませんでした。この問題を修正しました。
- ・ (HUB-35075)。Chromeブラウザで構成表ページをPDFに保存しようとする、表示の問題が発生していました。この問題を修正しました。
- ・ (HUB-35092、HUB-35171、HUB-36088)。APIリクエストを使用して、アーカイブ済みフェーズのプロジェクトまたはバージョンにコンポーネントを追加または削除すると、200 OK応答が返されていましたが、実際にはコンポーネントは追加も削除もされていませんでした。この問題を修正しました。現在では、この操作でエラーが表示されるようになりました。またUIには、削除オプションが表示されなくなります。
- ・ (HUB-35773、HUB-37305)。バイナリ スキャンの結果、1個のファイルが複数のコンポーネントにマッチしていた場合でも、構成表の[ソース]タブには1個のコンポーネントのみが表示されていました。この問題を修正しました。
- ・ (HUB-35836)。プロジェクトからプロジェクト所有者を削除した際に、Black Duckではプロジェクトが孤立したプロジェクトになることを防止できませんでした。この問題を修正しました。このアクションの実行を防止するために、直接アクセスユーザーの割り当てチェックが追加されました。
- ・ (HUB-36108)。QuartzSnippetScanAutoBomJobが原因で、スニペットスキャンの実行に時間がかかって、タイムアウトが発生していました。この問題を修正しました。
- ・ (HUB-36351)。カスタムコンポーネントバージョンの更新とカスタムコンポーネントバージョンの作成に関して、APIドキュメントを修正しました。
- ・ (HUB-36387)。修正ステータス更新時に、API経由で特定の脆弱性に緩和策を適用した場合に緩和策は適用されるが、riskPriorityDistributionには一部の緩和策が反映されないという並列性の問題が発生していました。この問題を修正しました。
- ・ (HUB-36446)。SigmaツールのダウンロードがHTTP 401 Unauthorizedメッセージで失敗する可能性があります。この問題を修正しました。
- ・ (HUB-36676)。OpenShift環境にPlatform One Black Duckをインストールしようすると、ファイル アクセス権の問題が発生していました。この問題を修正しました。
- ・ (HUB-36716)。BDSAで自動修正されたはずの脆弱性が、新しいプロジェクトバージョンまたはクローンでは、無視されたコンポーネントとして表示され、この表示から除外されませんでした。この問題を修正しました。

- ・ (HUB-36719)。サブプロジェクトを親プロジェクトに追加する際に、[通知ファイルレポートに含める]チェックボックスをオフにしても、通知レポートには件名が含まれていました。この問題を修正しました。件名のこのチェックボックスをオフにすると、現在では、プロジェクト階層内で上位の全プロジェクトからサブプロジェクトが除外されるようになりました。
- ・ (HUB-36763)。ユーザーが設定したプロキシが原因でSigmaToolStoreStateCheckAndRetryJobが失敗する可能性があります。この問題を修正しました。プロキシを使用していないときはsig-repoにアクセスできないが、プロキシを使用しているときはアクセスできる場合、ジョブは失敗しなくなりました。
- ・ (HUB-36905)。単一のリーフファイルに署名スキャンを実行すると、Nullポインタ例外エラーが発生する可能性があります。この問題を修正しました。
- ・ (HUB-36952)。ファイルおよびパッケージの調整操作でNullポインタ例外を修正しました。
- ・ (HUB-37031)。MaaSが有効な場合に、マッチ数の不一致が発生し、matched-files応答にURIプロパティが挿入されなくなっていました。この問題を修正しました。
- ・ (HUB-37078)。複数のUIページで、何度もクリックしないとブラウザの[戻る]ボタンが機能しないという問題が発生していました。この問題を修正しました。
- ・ (HUB-37109)。製品では、スニペットマッチの使用を設定する機能は現在サポートされていないため、この機能を削除しました。他のすべてのマッチタイプでは、設定機能を使用できます。
- ・ (HUB-37232)。ライセンス、ライセンス参照、著作権のソースコードをアップロードして、ディスカバリを開く際に、自動スクロールが機能しないことがありました。この問題を修正しました。
- ・ (HUB-37233)。「要求された構成表コンポーネント表現の特定サブセット」の説明にある「構成表コンポーネント表現」リンクの移動先が、「構成表コンポーネント表現」ではなく、「構成表コンポーネントバージョン表現」に設定されていました。このREST APIドキュメントの問題を修正しました。
- ・ (HUB-37308)。スキャンリストページのスキャンサイズにスニペットスキャンサイズが含まれて、両方の総合計が誤って表示されていました。この問題を修正しました。
- ・ (HUB-37312)。オブジェクトを検索した際に、マウントしたストレージボリューム内に/opt/blackduck/hub/uploads/toolsディレクトリが存在しなかった場合、「Unable to access tool」エラーが発生する可能性があります。この問題を修正しました。
- ・ (HUB-37414)。プロジェクト構成表ページのスキャンステータスが処理中の状態で停止し、ページの再読み込みだけでもステータスが更新されていました。この問題を修正しました。
- ・ (HUB-37439)。スニペットとマッチするパスの長さが非常に長くなり、スニペットビューではパスの一部が見えなくなっていました。この問題を修正しました。
- ・ (HUB-37453)。プロジェクト バージョン ページにフィルタを適用した場合に、ページを再読み込みした後、またはこのページから移動した後では、ページの表示内容が変わっていました。この問題を修正しました。
- ・ (HUB-37505)。「[ジョブ]」ページ(/api/jobs)では、ジョブが正しい順序で表示されませんでした。この問題を修正しました。現在、ジョブは終了時刻により降順でリストされます。
- ・ (HUB-37554)。component/パラメータを指定した/api/projects/<id>/versions/<id>/components/<id>/versions/<id> APIリクエストを使用すると、componentVersionが見つからず、エラーが発生していました。この問題を修正しました。不明なバージョンを持つようにコンポーネントを設定するには、componentVersionフィールドを空の文字列""に設定します。
- ・ (HUB-37648)。バイナリ スキャン (BDDBA統合) で、[コンポーネント]タブと[コンポーネント]レポートに複数のコンポーネントが表示されている場合でも、[ソース]タブと[ソース]レポートでは各バイナリ ファイルの1コンポーネント マッチのみが表示されていた問題を修正しました。
- ・ (HUB-37661)。構成表が別のプロジェクトを参照している場合に、[セキュリティ]タブに空白のロード領域が表示されることがありました。この問題を修正しました。

- ・ (HUB-37696)。コンポーネントのURLを含むコメントが適切に改行されず、画面に表示されないことがありました。この問題を修正しました。セキュリティ上の理由により、リンクはプレーンテキストで表示されます。リンク先に移動する場合は、リンクをコピーペーストする必要があります。
- ・ (HUB-37757)。「[スキャン]」ページの「[削除]」ボタンは、使用後にページが期待どおりに再読み込みされないため、使用後に機能しなくなることがありました。この問題を修正しました。
- ・ (HUB-37775)。編集オプションを使用して、コンポーネントの取得元を手動で追加しようとすると、取得元IDのパスが部分的に表示されないことがありました。この問題を修正しました。
- ・ (HUB-37789)。ソース ツリー ビューで、マッチしたファイル/フォルダの名前をコピーできなくなることがありました。この問題を修正しました。
- ・ (HUB-37925)。「[概要]」タブのオプションでプロジェクトをフィルタリングした後、UIでフィルタを削除できないことがありました。この問題を修正しました。

Black Duck 2023.1.x

Black Duck バージョン2023.1.2

- ・ [発表](#)
- ・ [新機能および変更された機能](#)
 - ・ [APIの機能強化](#)
 - ・ [バイナリスキャナ情報](#)
 - ・ [修正された問題](#)

発表

プロジェクトバージョンの自動削除機能を更新しました

Black Duck 2023.1.0では、プロジェクト バージョンの自動削除機能（以前は自動データ削除と呼ばれていました）が更新されました。リリース2023.1.0以降にアップグレードすると、この機能はデフォルトで有効になります。

プロジェクト バージョンの自動削除機能を使用すると、Black Duck内の古いプロジェクト バージョンを自動で削除できます。デフォルト設定では、更新またはスキャンが90日間実行されていないプロジェクトバージョンが削除されます。2023.1.xにアップグレードした場合、更新または再スキャンが45日間実行されなかった古いプロジェクトバージョンは、アップグレードの45日後に削除されます（アップグレード後も再スキャンまたは更新がなかった場合）。これらの設定は、システム管理者のデータ保持設定ページで変更できます。

新機能および変更された機能

新しい自動OAuthトークン更新

Black Duck は、GitLabとBitbucketのアクセストークンが期限切れになった後、これらを自動で再生成するようになりました。

ヒートマップ機能の強化

「開始済み」状態のスキャンがヒートマップUIメトリックに含まれるようになりました。

APIの機能強化

Black Duck 2023.1.2には、新規のまたは変更されたAPIリクエストはありません。APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

バイナリスキャナ情報

Black Duck 2023.1.2のバイナリ スキャナには、新機能や変更された機能はありません。

修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (HUB-35747)。特定の定期的ジョブ (BomAggregatePurgeOrphansJob、KbUpdateWorkflowJob) の終了がブロックされる問題を修正しました。
- ・ (HUB-36781)。KubernetesまたはOpenShiftでカスタムfsGroupを使用した場合に、Black Duckバージョン2022.10.xをインストールできない可能性があった問題を修正しました。
- ・ (HUB-36796)。ユーザーをプロジェクトグループに直接割り当て、同じユーザーをプロジェクトグループに割り当てられているユーザーグループにも割り当てると、複数のプロジェクトグループがAPIによって返されてDetectが失敗していた問題が修正されました。
- ・ (HUB-36939)。システム管理者としてBlack Duckにログインすると、デバッグ ページでパスワードがプレーン テキストで表示される問題を修正しました。
- ・ (HUB-36997)。オンプレミスKnowledgeBaseを使用して生成された通知ファイルのライセンス情報が消失していた問題を修正しました。
- ・ (HUB-37143)。コンポーネントのバージョンが不明な場合、ポリシーの式「Newer Versions Count」を評価する高速スキャンが内部エラーで失敗する問題を修正しました。
- ・ (HUB-37285)。デフォルトの管理者ユーザー名が変更された場合に、外部データベースを使用してBlack Duck 2023.1.0を新規にインストールすると失敗する可能性がありました。この問題を修正しました。
- ・ (HUB-37312)。オブジェクトを検索した際に、マウントしたストレージ ボリューム内に/opt/blackduck/hub/uploads/toolsディレクトリが存在しなかった場合に、Unable to access toolエラーが発生する可能性がありました。この問題を修正しました。

Black Duck バージョン2023.1.1

- ・ [発表](#)
- ・ [新機能および変更された機能](#)
 - ・ [APIの機能強化](#)
 - ・ [バイナリスキャナ情報](#)
 - ・ [修正された問題](#)

発表

Black Duck 2023.1.1に関する新たな発表はありません。

新機能および変更された機能

Black Duck 2023.1.1には、新機能や変更された機能はありません。

APIの機能強化

Black Duck 2023.1.1には、新規のまたは変更されたAPIリクエストはありません。APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

バイナリスキャナ情報

バイナリ スキャナがバージョン2022.12.0に更新されました。このバージョンには、Black Duckとのネットワーク通信回復性を向上する新しい再試行ポリシーおよび修正が含まれます。これは、統合されたバイナリ スキャンの信頼性を確保する、スキャン容量リソース制限の拡大に対応するためです。

修正された問題

このリリースでは、次の問題が修正されています。

- ・ (HUB-37171)。暗号化が有効なときは、認証コンテナがオンラインになりませんでした。この問題を修正しました。

Black Duck バージョン2023.1.0

- ・ [発表](#)
- ・ [新機能および変更された機能](#)
 - ・ [APIの機能強化](#)
 - ・ [バイナリスキャナ情報](#)
 - ・ [修正された問題](#)

発表

オブジェクトストレージサービスに関するシステムリソース要件の増加

Black Duck 2023.1.0では、オブジェクト ストレージ サービスを展開するための最小システム リソース要件が増加しました。オブジェクトストレージサービスには、さらにCPUを1つ、1 GBメモリ、および10 GBのディスク領域を追加する必要があります。これらの要件は今後のリリースで随時変更されることに注意してください。

データベースオブジェクト所有権の変更

blackduck(または、指定されている場合、ユーザー指定の代替所有者)によって所有されているデータベースオブジェクト(テーブル、ビューなど)は、所有権がblackduck_user(または、指定されている場合、ユーザー指定の代替所有者)に変更されました。

Helm2のサポート終了

Black Duck は、Kubernetes導入用のHelm2をサポートしなくなりました。サポートされているKubernetesの最小バージョンは1.13(Helm3でサポートされている最も古いバージョン)に引き上げられました。

ドキュメントのローカライゼーション

UI、オンラインヘルプ、およびリリースノートのバージョン2022.10.0が日本語と簡体字中国語にローカライズされました。

新機能および変更された機能

SCM統合の更新 - フェーズ3

Black Duck 2023.1.0では、SCM統合のリストに2つの新しいSCMプロバイダが追加されました。

- ・ [GitLab Self-Managed](#)
- ・ [Bitbucket Data Center](#)

これらの承認済みSCMプロバイダを追加できるようになりました。これらのプロバイダは、追加後、新しいプロジェクトの作成時に選択できます。これを実行すると、新しいプロジェクトの[プロジェクト設定]ページにリポジトリURLとブランチバージョンが自動的に入力されます。

この機能はDetect 8.x以降と互換性があり、新しいパッケージマネージャスキャンで有効になります。

SCM統合はBlack Duckではデフォルトでは有効になっておらず、環境に以下を追加して有効にする必要があります。

Swarmユーザーの場合は、blackduck-config.envファイルに以下を追加します。

```
blackduck.scan.scm.enableIntegration=true
```

Kubernetesユーザーの場合は、values.yamlファイルのenvironsセクションに以下を追加します。

```
environs:
    blackduck.scan.scm.enableIntegration: "true"
```

プロジェクトバージョンの自動削除の更新

プロジェクトバージョンの自動削除(旧「自動データ削除」)は、Black Duckユーザーインターフェイスで管理されるようになりました。これを行うには、[管理者] > [システム設定] > [データ保持]の順にクリックします。

署名スキャン処理中のファイルサイズの解析および集約の強化

過度に大きいスキャンでマッチエンジンサービスが停止しなくなり、代わりに、計算されたサイズが登録された制限よりも大きいというエラーとともにスキャンが失敗します。計算されたサイズは、次のいずれかです。

- ・ スキャンが登録制限内にある場合は、スキャンのフルサイズ。
- ・ 登録制限を超えた直後は、最後に計算されたスキャンサイズ。スキャンサイズの計算は、ライセンス制限をすでに超えている場合は続行しません。

ステートレス署名スキャン(従来の短期署名スキャン)

ステートレススキャンは、Black Duck内に永続的なストレージを作成も使用もしない、新しいスキャンモードです。このため、構成表(BOM)は保存されません。これは、指定されたスキャンターゲット内のポリシー違反をすばやく検出するために使用されます。ステートレススキャンを使用するには、次を実行する必要があります。

- ・ Black Duck Detect 8.2.0以降
- ・ Black Duck 2022.10.0以降
- ・ ホストされたナレッジベース
- ・ Match as a Serviceの有効化

Docker Swarmシークレットの暗号化のサポートを追加

Black Duck は、Docker Swarmシークレットの暗号化のサポートを追加しました。これにより、パスワード、SSH秘密キー、SSL証明書、または他のデータなど、データを一元管理し、アクセスを必要とするコンテナへのみ安全に送信できます。

アプリケーションレベルの暗号化とキーローテーションの追加

バージョン2023.1.0以降、Blackduckは、システム内で重要なデータ(Git SCM OAuthトークン、Gitアプリシークレット、SAMLプライベート署名キー、LDAP認証情報など)の暗号化をサポートします。この暗号化は、オーケストレーション環境(Docker SwarmまたはKubernetes)によってBlackduckインストールにプロビジョニングされたシークレットに基づいています。

新しい[コンポーネントインサイト]ページ

スキャンで見つかった特定のコンポーネントには、コンポーネントの取得元に関する追加情報を特定するのに役立つ、追加の詳細がある場合があります。[コンポーネントインサイト]ページでは、コンポーネントがどのように動作しているか、およびどのような機能が提供されるかについて理解を深めることができます。コンポーネントに追加のイ

ンサイトがある場合は、プロジェクトバージョンのページに移動し、そのコンポーネントのオプションメニューで[インサイト]を選択することで、コンポーネントを表示できます。

プロジェクトグループの新しいSBOMレポートフィールド

プロジェクトグループに新しいSBOMフィールドを追加して、ソフトウェア構成表(SBOM)レポートにその他の詳細を含めることができるようになりました。

- ・ 作成者:SPDXファイルを作成した個人または組織(電子メールアドレスを含む)。
- ・ 作成者のコメント:SPDXファイルの作成者が、SPDXファイルの作成に関する一般的なコメント、または他のフィールドに含まれないその他の関連コメントを入力するためのオプションフィールド。

新しいKBライセンス更新ジョブおよびセキュリティ更新ジョブ

現在のKB更新ジョブは、KBセキュリティ更新ジョブとKBライセンス更新ジョブに分割されます。KBライセンス更新ジョブは、デフォルトで毎日実行されるようにスケジュールされており、ジョブの頻度を変更するように構成できます。また、次のシステムプロパティを使用して、必要に応じてジョブを無効にすることができるように構成することもできます。

- ・ KB_LICENSE_UPDATER_PERIOD_MINUTES: ジョブの頻度を分単位で設定します。
- ・ KB_UPDATE_JOB_ENABLED: falseに設定すると、セキュリティ更新ジョブとライセンス更新ジョブの両方が無効になります。

SBOMレポートのreferenceLocator URLの更新

SBOMレポートのreferenceLocatorフィールドには、URLではなく、Black Duck KBの一意のIDのみが表示されるようになります。

高速スキャン機能の強化

Black Duck 2021.10.0は、プロジェクトグループで定義されたポリシールールを導入しました。これにより、お客様は、フルスキャンモードでのみ使用できた特定のプロジェクトグループでポリシールールをスコーピングできます。Black Duck 2023.1.0では新しく、プロジェクトグループベースのポリシーが、高速スキャンモードでサポートされるようになりました。

高速スキャンユーザーは、次のDetect/パラメータを使用して、スキャンされたプロジェクトの親プロジェクトグループを指定できます。

```
--detect.project.group.name=<project group name>
```

- ・ プロジェクトグループ名は、Black Duckの既存のプロジェクトグループと正確にマッチする必要があります。
- ・ <プロジェクトグループ名>は、指定されていても、プロジェクトがBlack Duckに存在しない場合、ポリシー決定のプロジェクトグループとして使用されます。

v3署名スキャン失敗処理の更新

2023.1.0以降では、コードの場所の制限またはスキャンしたコードの合計の制限を超えるすべてのv3署名スキャンは、イングレス後ではなく作成時に失敗します。失敗は、Black Duck UIには表示されず、代わりにスキャンクライアントに表示されます。

検索に関連するパフォーマンスの改善

Black Duckでの検索では、データベース内のマテリアライズドビューが使用されます。このビューは、検索結果が高速になるように定期的に更新されます。ただし、このビューの更新は、大規模なデータベースで問題が発生していま

した。当社は、すべてのフィルタを分析し、いくつかのフィルタが不要であると判断しました。さまざまな検索カテゴリから、当社は次のフィルタを削除しました。

プロジェクトバージョン検索

- ・ 配布
- ・ 階層

コンポーネント検索

- ・ ポリシールール
- ・ ポリシー違反の重大度
- ・ コンポーネント承認ステータス
- ・ レビューステータス
- ・ 脆弱性報告済み
- ・ 脆弱性CWE

脆弱性検索

- ・ ベーススコア
- ・ 攻撃される可能性のサブスコア
- ・ 影響サブスコア
- ・ 一時サブスコア
- ・ 到達可能

保存済みの検索は、これらのフィルタを削除する移行スクリプトを介して更新されます。ブックマークが設定された検索結果は、引き続き機能します。ただし、削除されたフィルタは無視されるため、結果はフィルタが選択されていないかようになります。削除されたフィルタのみで構成された、保存済みの検索は、完全に削除されます。

新しいスキャンヒートマップ

過去30日間の特定の日、時刻に実行されたスキャンの合計数を表示するオンデマンドヒートマップを表示できるようになりました。色分け表示されたマトリックスには、最小/最大の関係に基づいてスキャンの合計数が表示されます。緑の値は低い値を示し、赤の値は高い値を示します。ヒートマップは、Black Duckで[管理者]ボタンをクリックしてから、[診断]セクションの[ヒートマップ]を選択することで確認できます。

新しいBlack Duckストレージコンテナ

Black Duck 2023.1.0では、静的ファイル(SBOMやその他のレポートなど)を永続ストレージに移動できる新しいストレージサービスが導入されました。このサービスにより、データベースの領域が解放され、スキャンパフォーマンスとスケーラビリティの強化が可能になっています。

レポートスキーマの変更

Black Duck 2023.1.0では、255文字を超えるパスに対応できるように、reporting.scan_viewのbasedir列のタイプがcharacter varyingからtextに変更されました。

新しいプロジェクトグループ管理者の役割

新しいプロジェクトグループ管理者の役割には、ローカルレベルでプロジェクトグループを管理する能力があります。たとえば、この管理者はプロジェクトグループを作成/編集/削除したり、親プロジェクトグループの下のプロジェクトグループからメンバーとユーザーグループを追加/削除したりできます。

サポートされるブラウザのバージョン

- ・ Safariバージョン16.2 (17614.3.7.1.7、17614)
 - ・ Safariバージョン13.0以前はサポートされなくなりました
- ・ Chromeバージョン109.0.5414.87 (公式ビルド) (x86_64)
 - ・ Chromeバージョン71以前はサポートされなくなりました
- ・ Firefoxバージョン109.0 (64ビット)
 - ・ Firefoxバージョン71以前はサポートされなくなりました
- ・ Microsoft Edgeバージョン109.0.1518.55 (公式ビルド) (64ビット)
 - ・ Microsoft Edgeバージョン78以前はサポートされなくなりました

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:13-2.15
- ・ blackducksoftware/blackduck-authentication:2023.1.0
- ・ blackducksoftware/blackduck-webapp:2023.1.0
- ・ blackducksoftware/blackduck-scan:2023.1.0
- ・ blackducksoftware/blackduck-jobrunner:2023.1.0
- ・ blackducksoftware/blackduck-cfssl:1.0.15
- ・ blackducksoftware/blackduck-logstash:1.0.26
- ・ blackducksoftware/blackduck-registration:2023.1.0
- ・ blackducksoftware/blackduck-nginx:2.0.31
- ・ blackducksoftware/blackduck-documentation:2023.1.0
- ・ blackducksoftware/blackduck-upload-cache:1.0.34
- ・ blackducksoftware/blackduck-redis:2023.1.0
- ・ blackducksoftware/blackduck-bomengine:2023.1.0
- ・ blackducksoftware/blackduck-matchengine:2023.1.0
- ・ blackducksoftware/blackduck-webui:2023.1.0
- ・ sigsynopsys/bdba-worker:2022.12.0
- ・ blackducksoftware/rabbitmq:1.2.15

APIの機能強化

APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

プロジェクトエンドポイントの強化

OSSコンポーネントのpURL座標を含むように、次のエンドポイントが更新されました:

- ・ `/api/projects/<projectId>/versions/<projectVersionId>/components`
- ・ `/api/projects/<projectId>/versions/<projectVersionId>/vulnerable-bom-components`
- ・ `/api/projects/<projectId>/versions/<projectVersionId>/components?filter=licensePolicy`

data-retention APIエンドポイントの更新

次のエンドポイントは、PUTリクエストからPATCHリクエストに変更されました：

- ・ `/api/settings/data-retention`

新しいツールリストAPIエンドポイント

使用可能なすべてのツールバージョンを一覧表示する新しいパブリックエンドポイントが使用可能になりました。

- ・ `/api/tools`

特定のプロジェクト グループに必要なSBOMフィールドの新規取得

新しいパブリック エンドポイントを使用し、プロジェクトのSBOMフィールドを読み取れるようになりました。

- ・ `/api/project-groups/{projectId}/sbom-fields`

バイナリスキャナ情報

バイナリ スキャナがバージョン2022.12.0に更新されました。このバージョンには、Black Duckとのネットワーク通信回復性を向上する新しい再試行ポリシーおよび修正が含まれます。これは、統合されたバイナリ スキャンの信頼性を確保する、スキャン容量リソース制限の拡大に対応するためです。

修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (HUB-32387)。redisがデフォルトのOpenShift環境でデータにアクセスできない問題を修正しました。
- ・ (HUB-33820)。構成表でコンポーネントが更新された(たとえば、KnowledgeBaseでのステータスが[レビュー済み]に設定された)後に警告が表示され、ユーザーがページを手動で再ロードするまで警告が消えないことがある問題を修正しました。
- ・ (HUB-34056)。[編集]ダイアログで[スニペットの調整と確認]をオンにしたときに個々のコンポーネント編集が一括のコンポーネント編集と異なる結果を表示する問題を修正しました。
- ・ (HUB-34374)。[プロジェクト バージョン]ページの[ソース]タブの[検出タイプ]列の値がフィルタと矛盾して表示されることがある問題を修正しました。
- ・ (HUB-34502)。無視されたコンポーネントをレポートに含めたとき、確認済みまたは未確認のスニペット結果がソース レポートに含まれない問題を修正しました。
- ・ (HUB-34596)。内部ユーザーと同じユーザー名を共有するSAMLユーザーを作成しようとすると、重複制約エラーが発生する問題を修正しました。
- ・ (HUB-34725)。バージョンレポートでFILE_DEPENDENCY_DIRECTエントリとFILE_DEPENDENCY_TRANSITIVEエントリが重複している問題を修正しました。
- ・ (HUB-34756)。APIを使用してプロジェクト グループを通じてユーザー グループのロールが割り当てられたときに、スコープが[サーバー]と表示される問題を修正しました。
- ・ (HUB-34947)。無視されたスニペットがSPDXレポートに表示されることがある問題を修正しました。
- ・ (HUB-35472)。synopsysctlでMAX_TOTAL_SOURCE_SIZE_MBの値の変更が正しく適用されない問題を修正しました。
- ・ (HUB-35557)。不適切な形式の/api/projects/リクエストがHTTP 4xxエラーコードではなくHTTP 5xxエラーコードを返す問題を修正しました。
- ・ (HUB-35585)。「更新者」のデータが更新されず、変更を行ったユーザーのユーザー名として「システム管理者」が常に反映され、古い日時が設定される問題を修正しました。
- ・ (HUB-35764)。トップメニューとスニペットウィンドウのGUIバグを修正しました。

- ・ (HUB-35912)。すべてのオプションが選択されているライセンスリスクフィルタが適用されたときに、確認済みになり、その後無視されたスニペットマッチが消える問題を修正しました。
- ・ (HUB-35914)。(–nの代わりに–zを使用している)system_check.shスクリプトの不正なフラグを修正しました。
- ・ (HUB-35927)。コンポーネントのCVE BDSAマッピングに変更があった場合に、自動修正機能によって修正ステータスおよびコメントが元に戻されない問題を修正しました。
- ・ (HUB-35945)。プロジェクト バージョンの[スキャン]ページの[スキャン サイズ]値に、メインの[スキャン]ページに表示されるコードの場所のサイズ値が含まれない問題を修正しました。
- ・ (HUB-36321)。プロジェクト ビューアのロールで、スニペットの[ソース]ビューの[編集]オプションが利用可能となっていた問題を修正しました。
- ・ (HUB-36382)。複数のスキャンを高速で連続して受信したときにエラーを生成するまれな競合状態を修正しました。
- ・ (HUB-36498)。CVEのレコードが多すぎる場合に、GET /api/vulnerabilities/<CVE RECORD>/affected-projectsがHTTP 400エラーコードを返すことがある問題を修正しました。
- ・ (HUB-36629)。高速スキャンでポリシールールに違反する、追加の脆弱性が報告されることがある問題を修正しました。
- ・ (HUB-36703)。Black Duck UIと/api/projects/{projectId}/versions/{projectVersionId}/matched-files APIリクエストのマッチ タイプが異なる問題を修正しました。詳細については、上記の「APIの機能強化」セクションを参照してください。
- ・ (HUB-36707)。プロジェクト名またはバージョン名のスペルに誤りがある場合に、高速スキャンがすばやくエラーで終了するのではなくタイムアウトすることがある問題を修正しました。

Black Duck 2022.10.x

Black Duck バージョン2022.10.3

- ・ [発表](#)
- ・ [新機能および変更された機能](#)
 - ・ [APIの機能強化](#)
 - ・ [バイナリスキャナ情報](#)
 - ・ [修正された問題](#)

発表

Black Duck 2022.10.3に関する新たな発表はありません。

新機能および変更された機能

Black Duck 2022.10.3 には、新機能や変更された機能はありません。

APIの機能強化

Black Duck 2022.10.3には、新規のまたは変更されたAPIリクエストはありません。APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

バイナリスキャナ情報

バイナリスキャナがバージョン2022.9.2に更新されました。このバージョンには、重大度が高である、CVE-2022-3602 およびCVE-2022-3786の脆弱性に対応する、OpenSSL 3.0.7へのアップグレードが含まれます。

修正された問題

このリリースでは、次の問題が修正されています。

- ・ (HUB-37171)。暗号化が有効なときは、認証コンテナがオンラインになりませんでした。この問題を修正しました。

Black Duck バージョン2022.10.2

発表

Black Duck 2022.10.2に関する新たな発表はありません。

新機能および変更された機能

Black Duck 2022.10.2には、新機能や変更された機能はありません。

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:13-2.13
- ・ blackducksoftware/blackduck-authentication:2022.10.2
- ・ blackducksoftware/blackduck-webapp:2022.10.2
- ・ blackducksoftware/blackduck-scan:2022.10.2
- ・ blackducksoftware/blackduck-jobrunner:2022.10.2
- ・ blackducksoftware/blackduck-cfssl:1.0.10
- ・ blackducksoftware/blackduck-logstash:1.0.21
- ・ blackducksoftware/blackduck-registration:2022.10.2
- ・ blackducksoftware/blackduck-nginx:2.0.28
- ・ blackducksoftware/blackduck-documentation:2022.10.2
- ・ blackducksoftware/blackduck-upload-cache:1.0.31
- ・ blackducksoftware/blackduck-redis:2022.10.2
- ・ blackducksoftware/blackduck-bomengine:2022.10.2
- ・ blackducksoftware/blackduck-matchengine:2022.10.2
- ・ blackducksoftware/blackduck-webui:2022.10.2
- ・ sigsynopsys/bdba-worker:2022.9.2
- ・ blackducksoftware/rabbitmq:1.2.14

APIの機能強化

APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

プロジェクトエンドポイントの強化

OSSコンポーネントのpURL座標を含むように、次のエンドポイントが更新されました:

- ・ `api/projects/<projectId>/versions/<projectVersionId>/components`
- ・ `api/projects/<projectId>/versions/<projectVersionId>/vulnerable-bom-components`
- ・ `api/projects/<projectId>/versions/<projectVersionId>/components?filter=licensePolicy`

バイナリスキャナ情報

バイナリスキャナがバージョン2022.9.2に更新されました。このバージョンには、重大度が高である、CVE-2022-3602 およびCVE-2022-3786の脆弱性に対応する、OpenSSL 3.0.7へのアップグレードが含まれます。

修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (HUB-35377)。未確認のスニペット/無視されたスニペットをレビューするときに、ソース ビューを除くBlack Duck内のあらゆる場所で、未確認のスニペットおよび無視されたコンポーネントが、コンポーネントまたはライセンスの使用回数に表示されていた問題を修正しました。
- ・ (HUB-35850)。RedisがデフォルトのOpenShift環境でデータにアクセスできない問題を修正しました。
- ・ (HUB-36049)。FileBackedOutputStream一時ファイルが、スキャンコンテナの下の/tmpディレクトリに書き込まれ、クリーンアップされない問題を修正しました。
- ・ (HUB-36149)。BOMをPDFとして印刷するときにプロジェクト名およびバージョン名が含まれない問題を修正しました。
- ・ (HUB-36359)。Githubリリースページでblackduck-webuiコンテナへのリンクが欠落している問題を修正しました。
- ・ (HUB-36495)。オンラインヘルプの古い画像を修正しました。

Black Duck バージョン2022.10.1

発表

OpenSSLバージョン3.0.0～3.0.6のセキュリティアドバイザリ

2022年11月1日、OpenSSL Projectは、OpenSSL 3.0.xに存在する、重大度が高である次の脆弱性を公開しました。

両方の脆弱性の性質により、X.509証明書検証、特に名前制約チェックでトリガーできるバッファオーバーランが可能になります。これは、証明書チェーン署名検証の後に発生することに注意してください。さらに、これは、CAが悪意のある証明書に署名していることを必要とすること、または信頼できる発行者へのパスを構築できなかったとしてもアプリケーションが証明書検証を続行することを必要とすることにも注意してください。

CVE-2022-3602: 攻撃者は、悪意のある電子メールアドレスを作成して、攻撃者が制御するスタック上の4バイトをオーバーフローさせる可能性があります。このバッファオーバーフローの結果、(サービス拒否の原因となる)クラッシュが発生したり、潜在的にリモートコード実行が発生したりする可能性があります。

CVE-2022-3786: 攻撃者は、証明書内に悪意のある電子メールアドレスを作成して、スタック上に「.」文字(10進数46)を格納して任意のバイト数をオーバーフローさせる可能性があります。このバッファオーバーフローの結果、(サービス拒否の原因となる)クラッシュが発生する可能性があります。

現在、Black Duckは、Black Duck SIGの製品、サービス、システムへの露出が制限されていると考えています。露出された範囲で、悪用を防止する緩和策を適用しています。

バイナリスキャナ(BDBA)がバージョン2022.9.2に更新されました。このバージョンには、重大度が高である脆弱性に対応する、OpenSSL 3.0.7へのアップグレードが含まれます。BDBAなしで2022.10.0を実行しているお客様は、アップグレードする必要はありません。

今後の更新については、[コミュニティページ](#)を引き続きご確認ください。

新機能および変更された機能

Black Duck 2022.10.1には、新機能や変更された機能はありません。

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:13-2.13
- ・ blackducksoftware/blackduck-authentication:2022.10.1
- ・ blackducksoftware/blackduck-webapp:2022.10.1
- ・ blackducksoftware/blackduck-scan:2022.10.1
- ・ blackducksoftware/blackduck-jobrunner:2022.10.1
- ・ blackducksoftware/blackduck-cfssl:1.0.10
- ・ blackducksoftware/blackduck-logstash:1.0.21
- ・ blackducksoftware/blackduck-registration:2022.10.1
- ・ blackducksoftware/blackduck-nginx:2.0.28
- ・ blackducksoftware/blackduck-documentation:2022.10.1
- ・ blackducksoftware/blackduck-upload-cache:1.0.29
- ・ blackducksoftware/blackduck-redis:2022.10.1
- ・ blackducksoftware/blackduck-bomengine:2022.10.1
- ・ blackducksoftware/blackduck-matchengine:2022.10.1
- ・ blackducksoftware/blackduck-webui:2022.10.1
- ・ sigsynopsys/bdba-worker:2022.9.2
- ・ blackducksoftware/rabbitmq:1.2.14

APIの機能強化

Black Duck 2022.10.1には、新規のまたは変更されたAPIリクエストはありません。APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

バイナリスキャナ情報

バイナリスキャナがバージョン2022.9.2に更新されました。このバージョンには、重大度が高である、CVE-2022-3602およびCVE-2022-3786の脆弱性に対応する、OpenSSL 3.0.7へのアップグレードが含まれます。

修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (HUB-36290)。OpenSSLの脆弱性に対応して、BDBAワーカーを更新しました。

Black Duck バージョン2022.10.0

2022.10.0の発表

PostgreSQL 11の廃止

PostgreSQL 11上におけるBlack Duckの実行に関するサポートは、2022.10.0リリースで終了しています。このリリース以降、PostgreSQL 11でBlack Duckを実行しようとするとエラーが発生し、Black Duckは起動しません。

PostgreSQL 13コンテナの移行

Black Duck 2022.10.0はPostgreSQLイメージをバージョン11からバージョン13に移行しており、PostgreSQL 9.6コンテナ(バージョン4.2から2021.10.xまで)またはPostgreSQL 11コンテナ(バージョン2022.2.0から2022.7.xまで)を使用し

たバージョンからのアップグレードをサポートしています。インストール中に、blackduck-postgres-upgraderコンテナは既存のデータベースをPostgreSQL 13に移行し、完了すると終了します。

コア以外のPG拡張機能を使用しているお客様の場合は、移行前にそれらをアンインストールし、移行が正常に完了した後に再インストールすることを強くお勧めします。そうしないと、移行が失敗する可能性があります。

レプリケーションを設定しているお客様は、移行前に、pg_upgradeのドキュメントの手順に従う必要があります。そこで説明されている準備が行われていない場合、移行はおそらく成功しますが、レプリケーションの設定が壊れます。

Black DuckのPostgreSQLイメージを使用していないお客様には影響はありません。

重要: 移行を開始する前に:

- ・ システムカタログのデータコピーによるディスクの使用に起因する予期しない問題を回避するため、10%ほどの余裕をディスク容量に確保してください。
- ・ ディスク容量が不足するとLinuxシステムが中断する可能性があるため、ルートディレクトリの容量とボリュームマウントを確認してください。

KubernetesおよびOpenShiftユーザーの場合:

- ・ プレーンなKubernetesでは、アップグレードジョブのコンテナはルートとして実行されます。ただし、唯一の要件は、ジョブがPostgreSQLデータボリュームの所有者と同じUIDで実行されることです。
- ・ OpenShiftでは、アップグレードジョブは、PostgreSQLデータボリュームの所有者と同じUIDで実行されることを前提としています。

Swarmユーザーの場合:

- ・ 移行は完全に自動化されているため、Black Duckの標準アップグレードの操作以外に追加の操作は必要ありません。
- ・ 上記のレイアウトとUIDの変更を行うには、blackduck-postgres-upgraderコンテナをルートとして実行する必要があります。
- ・ その後のBlack Duckの再起動時に、blackduck-postgres-upgraderは移行が不要であると判断し、すぐに終了します。

データベースbds_hub_reportの廃止

Black Duck 2021.10.0のリリース ノートに記載されているように、Black Duckの新規インストールではbds_hub_reportデータベースは作成されません。2022.10.0では、bds_hub_reportデータベースが削除されます。

bds_hub_reportデータベースを保存したいユーザーは、hub_create_data_dump.shスクリプトを使用してbds_hub_reportデータベースをダンプできます(ある場合)。

2022年11月のBlack Duck KnowledgeBase IPアドレス変更に関する通知

2022年11月14日の週に、Black Duck KnowledgeBase(<https://kb.blackducksoftware.com>)のIPアドレスが変更されます。この14日の週の間は、DNSを更新して新しいIPアドレスにトラフィックが転送されるようにします。ほとんどのお客様は何もする必要はありません。

IP許可リストを使用してKBと通信するオンプレミスのお客様は、ファイアウォールを更新し、許可リストにこれらの新しいIPアドレスを含める必要があります。トラフィックまたはIP許可リストを制限するためにファイアウォールルールを使用しないお客様は影響を受けません。

IPアドレスを使用しているお客様の場合、リストを許可するために次のIPアドレスを追加する必要があります。

NAM(北米)

kb-na.blackducksoftware.com: 34.160.126.173

EMEA(ヨーロッパ、中東、アフリカ)

kb-emea.blackducksoftware.com: 34.149.112.69

APAC(アジア太平洋、アジア、中国)

kb-apac.blackducksoftware.com: 34.111.46.24

この変更は、IPアドレスの更新を自動的に処理するため、DNS解決を使用する大部分のお客様には影響しません。IPアドレス許可リストを使用しているお客様は、次の3つの新しいIPアドレスを許可リストに追加する必要があります。34.160.126.173、34.149.112.69、34.111.46.24。

現在のIPアドレス(参照用)は次のとおりです。

NAM: 35.224.73.200

EMEA: 35.242.234.51

APAC: 35.220.236.106

この変更は、可用性の高い安全なKBを提供するための継続的な取り組みの一環として行われています。

サーバー移行後に質問がある場合や問題が発生した場合は、[サポートケースを提出](#)してください。

オブジェクトストレージサービスの今後のシステムリソース要件

Black Duck 2023.1.0では、オブジェクト ストレージ サービスを展開するための最小システム リソース要件が増加します。オブジェクトストレージサービスには、さらにCPUを1つ、1 GBメモリ、および10 GBのディスク領域を追加する必要があります。これらの要件は今後のリリースで随時変更されることに注意してください。

ドキュメントのローカライゼーション

UI、オンラインヘルプ、およびリリースノートのバージョン2022.7.0が日本語と簡体字中国語にローカライズされました。

2022.10.0の新機能および変更された機能

GitリポジトリSCM統合 - フェーズ2

Black Duck 2022.10.0では、プロジェクトとバージョンの作成時にユーザーがリポジトリまたはブランチ フィールドを追加できるようになりました。承認されたSCMプロバイダ (GitHub StandardおよびGitHub Enterpriseのみ)を追加できるようになりました。この機能は、新しいプロジェクトを作成するときに選択できます。これを実行すると、新しいプロジェクトの[プロジェクト設定]ページにリポジトリURLとブランチバージョンが自動的に入力されます。

この機能はDetect 8.x以降と互換性があり、新しいパッケージマネージャスキャンで有効になります。

SCM統合はBlack Duckではデフォルトでは有効になっておらず、環境に以下を追加して有効にする必要があります。

Swarmユーザーの場合は、blackduck-config.envファイルに以下を追加します。

```
blackduck.scan.scm.enableIntegration=true
```

Kubernetesユーザーの場合は、values.yamlファイルのenvironsセクションに以下を追加します。

```
environs:
  blackduck.scan.scm.enableIntegration: "true"
```

プロジェクトバージョンコンポーネントでの新しい一括アクション

一括更新機能では、プロジェクトバージョンページのコンポーネントで次のアクションがサポートされるようになりました。

1. コンポーネントを無視/無視解除する
2. コンポーネントの使用法の種類を設定する
3. レビュー済み/未レビューとしてマークする
4. 通知ファイルに包含/除外を設定する

構成表にUTF8を使用したレポートの作成

この機能はBlack Duck 2022.7.0で追加されましたが、同バージョンのリリース ノートから誤って省略されていることに注意してください。

Black Duck 2022.7.0では、アルファベット以外の文字を使用しているお客様向けのレポートで、構成表の文字エンコードにUTF8のサポートが導入されました。この機能を有効にするには、blackduck-config.envファイルに以下を追加します。

```
USE_CSV_BOM=true
```

新しいヒートマップデータのダウンロード

ヒートマップを圧縮CSVとしてダウンロードして端末スキャンの傾向を確認および分析し、スプレッドシートプログラムのピボットとしてヒートマップを作成することができるようになりました。このデータをダウンロードするには、[管理者] > [診断] > [システム情報]の順に移動します。

新しいSBOMレポートフィールド

プロジェクトに新しいSBOMフィールドを追加して、ソフトウェア構成表 (SBOM) レポートに詳細を含めることができるようになりました。SBOMフィールドには、次の新しいフィールドがあります。

構成表コンポーネントレベルでの設定:

- ・ パッケージURL: SPDXレポートのreferenceCategory: PACKAGE_MANAGER要素のreferenceType: purlとしてexternalRefsセクションにリストされ、CycloneDXレポートのpurlとしてcomponentsセクションの下にリストされます。
- ・ パッケージサプライヤ: 両方のレポートタイプに対して、(supplier)としてリストされます。
- ・ CPE: SPDXレポートのreferenceCategory: SECURITY要素のreferenceLocatorとしてexternalRefsセクションにリストされ、CycloneDXレポートのcpeとしてcomponentsセクションの下にリストされます。

コンポーネントレベルでの設定:

- ・ 説明: 両方のレポートタイプに対して、(description)としてリストされます。
- ・ 発信者: SPDXレポートのpackagesセクションの下にoriginatorとしてリストされ、components CycloneDXレポートの下にauthorとしてリストされます。

新しいグローバル通知ビューアの役割

すべてのプロジェクトへの読み取り専用アクセス権を持ち、ユーザー設定に関係なくすべてのシステム通知を受信できる新しい役割が作成されました。

新しい通知サブスクリプション管理

ユーザーが受信する通知を有効または無効にすることができるようになりました。これらの設定を管理するには、[管理] > [システム設定] > [通知]の順に選択します。グローバル通知ビューアの役割を持つユーザーは、システム上のすべての通知を引き続き受信します。

更新されたウォッチするプロジェクトの通知管理

[マイ設定]ページで、通知を受信するウォッチするプロジェクトを管理できるようになりました。これを実行するには、右上のメニューでユーザー名をクリックし、[ウォッチするプロジェクト]をクリックして、[ウォッチするプロジェクト]タブを選択します。

更新された通知保持期間

通知保持のデフォルト設定値は、30日間から14日間に短縮されました。これは、blackduck-config.envでBLACKDUCK_HUB_NOTIFICATIONS_DELETE_DAYS環境変数を設定することによって実行できます。

ポリシーの新しい脆弱性条件

新しい脆弱性タグのカテゴリがリモートコード実行(RCE)の脆弱性を置換して含めるポリシーの脆弱性条件に追加されました。このカテゴリには、ポリシーの作成時または編集時に次のフィルタオプションが含まれます。

- ・ ゼロクリックリモートコード実行: システム上でコードが実行される可能性がある脆弱性。第三者のアクションを必要とせずに、リモートの攻撃者によってトリガーされます。
- ・ 特定された悪意のあるコード: 悪意のあるコードを含むソフトウェア。システム内で実行された場合、有害または破壊的な結果をもたらすように設計されています。
- ・ 開示禁止脆弱性の詳細: 現在、技術的詳細が開示禁止中であり、現時点ではベンダーから詳細が公開されていない脆弱性。
- ・ 未確認の脆弱性: ベンダーが、コンポーネントの動作が意図したものであり、脆弱性が存在しないと判断したために、コードベースの修正が行われていない脆弱性。

脆弱性更新レポートに新しい脆弱性タグが追加されました

脆弱性更新レポートに脆弱性タグが表示されるようになりました(該当する場合)。これらのレポートには、上記の脆弱性タグが含まれます。

リストと表の新しいエクスポート機能

次のページでリストと表をCSVにエクスポートできるようになりました。

- ・ [ダッシュボード]ページ: ダッシュボードの[結果の概要]セクションにあります。
- ・ [検索]ページ: [検索]ページの左側にある検索フィールドの上にあります。
- ・ [スキャン]ページ: [スキャン]ページの左上にある[削除]ボタンの横にあります。
- ・ [ユーザーとグループ]ページ: [ユーザーとグループ]ページの左上にある[ユーザーの作成]ボタンの横にあります。

バイナリスキャンおよびProtex構成表インポート用にBDIOをインポートする際に強化されたソースビュー

現在、[スキャン]ページには、構成表インポートログに見つからないコンポーネントがリストされます。2022.10.0リリースでは、マッチしないコンポーネントも[ソースビュー]タブに表示されます。マッチしないコンポーネントは、新規スキャンの場合にのみソースビューに表示されることに注意してください。既存のスキャンは変更されません。

レポートスキーマの機能強化

reporting.componentビューに、次の3つのフィールドが追加されました。

- ・ reporting.component.created_at: コンポーネントの作成時に、構成表からコピーされました。コンポーネントが初めて構成表に追加されたことを表します。
- ・ reporting.component.updated_at: コンポーネントの更新時に、構成表からコピーされました。コンポーネントが構成表で更新された最新の時刻を表します。

- ・ `reporting.user_group_project_mapping`: どのユーザーがどのグループ(複数の場合あり)にマッピングされ、どのユーザーがどのプロジェクト(複数の場合あり)にマッピングされているかを追加します。

新しい短期署名スキャン - お客様の使用の制限

短期署名スキャンは、Black Duck内に永続的なストレージを作成も使用もしない、新しいスキャン モードです。このため、構成表(BOM)は保存されません。これは、指定されたスキャンターゲット内のポリシー違反をすばやく検出するために使用されます。一時署名スキャンを使用するには、次を実行している必要があります。

- ・ Black Duck Detect 8.2.0以降
- ・ Black Duck 2022.10.0以降
- ・ ホストされたKnowledgeBase
- ・ Match as a Serviceの有効化

この機能には使用制限があるため、Black Duck 2022.10.0では一般的には利用できません。

Synopsysctlの更新

Black Duckctlは新しいPostgreSQL 13コンテナで動作するよう更新されました。

コンテナバージョン

- ・ `blackducksoftware/blackduck-postgres:13-2.13`
- ・ `blackducksoftware/blackduck-authentication:2022.10.0`
- ・ `blackducksoftware/blackduck-webapp:2022.10.0`
- ・ `blackducksoftware/blackduck-scan:2022.10.0`
- ・ `blackducksoftware/blackduck-jobrunner:2022.10.0`
- ・ `blackducksoftware/blackduck-cfssl:1.0.10`
- ・ `blackducksoftware/blackduck-logstash:1.0.21`
- ・ `blackducksoftware/blackduck-registration:2022.10.0`
- ・ `blackducksoftware/blackduck-nginx:2.0.28`
- ・ `blackducksoftware/blackduck-documentation:2022.10.0`
- ・ `blackducksoftware/blackduck-upload-cache:1.0.29`
- ・ `blackducksoftware/blackduck-redis:2022.10.0`
- ・ `blackducksoftware/blackduck-bomengine:2022.10.0`
- ・ `blackducksoftware/blackduck-matchengine:2022.10.0`
- ・ `blackducksoftware/blackduck-webui:2022.10.0`
- ・ `sigsynopsys/bdba-worker:2022.9.1`
- ・ `blackducksoftware/rabbitmq:1.2.14`

APIの機能強化

APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

新しいスキャン監視APIエンドポイント

新しいREST APIエンドポイントが追加されました。このエンドポイントを使用してスキャンのエラー率を分析し、指定された時間内にシステムの端末スキャンからスキャン監視情報を取得できます(デフォルトは過去1時間に設定されています)。

- GET /api/scan-monitor

リクエストパラメータは次のとおりです。

- level (必須)。数値1または2(デフォルトは1)。
リクエストの例: GET /api/scan-monitor?level=1

障害発生率が設定された最大しきい値(デフォルトは30%)を超えた場合、レベル1は単純なバイナリ応答OKまたはNOT OKです。

レベル2は、ステータスに応じて16進数のカラーコード(緑、黄、赤)を返します。緑色(#00FF00)は、監視対象時間(デフォルトでは過去1時間)の障害発生率が、設定されている最小しきい値(デフォルトは10%)を下回っていることを示します。黄色(#FFFF00)は、障害発生率が最小しきい値と最大しきい値(10%~30%)の間にあることを示します。赤色(#FF0000)は、障害発生率が最大しきい値(30%)を超えていることを示します。

カスタムフィールドのnull値の処理の向上

次のパブリックAPIリクエストは、カスタムフィールド値がnullの場合にエラーメッセージを返すよう更新されました。

- PUT /api/projects/{projectId}/custom-fields/{customFieldId}
- PUT /api/projects/{projectId}/versions/{projectVersionId}/custom-fields/{customFieldId}
- PUT /api/components/{componentId}/custom-fields/{customFieldId}
- PUT /api/components/{componentId}/versions/{componentVersionId}/customfields/{customFieldId}
- PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/custom-fields
- PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/custom-fields/{customFieldId}
- PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/custom-fields
- PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/custom-fields/{customFieldId}

通知エンドポイントの更新

次のREST APIパブリックエンドポイントが更新され、ユーザーがサブスクリプションの通知を受信する必要があるかどうかに基づいてnotifyUserフィールドが返されます。

- GET /api/users/{userId}/notification-subscriptions/{subscriptionId}
- GET /api/users/{userId}/notification-subscriptions

新しい構成表ステータスのエンドポイント

特定のスキャンに対して構成表が更新されたタイミングを判断するために、新しいREST APIエンドポイントが作成されました。

- GET /api/projects/{projectId}/versions/{versionId}/bom-status/{scanId}

ステータス値には、NOT_INCLUDED、BUILDING、SUCCESS、FAILUREがあります。

PUT /api/settings/auto-remediate-unmappedの廃止

Black Duck 2022.4.1では、パブリック エンドポイントPUT /api/settings/auto-remediate-unmappedはPATCH /api/settings/auto-remediate-unmappedに変更されましたが、PUTエンドポイントは廃止されており、下位互換性を維持するために保持されています。現時点でのリリースでは、PUT /api/settings/auto-remediate-unmappedエンドポイントが削除されました。

ライセンスAPIリクエストの廃止と削除

次のAPIリクエストは削除されました。

- GET /api/licenses/{licenseId}/obligations
- GET /api/licenses/{licenseId}/obligations-filters

GET api/licenses/{licenseId}/obligationsが削除されたため、必須のAPIはどのAPIからも返されなくなります。代わりに、ライセンス条項API(/api/licenses/{licenseId}/license-terms)が返されます。

また、次のAPIリクエストは廃止予定です。

- GET /api/licenses
- POST /api/licenses
- GET /api/licenses-filters
- GET /api/licenses/{licenseId}
- PUT /api/licenses/{licenseId}
- GET /api/licenses/{licenseId}/text
- PUT /api/licenses/{licenseId}/text

新たに強化されたコンポーネントエンドポイント

コンポーネントレベルでSBOMフィールド値を取得/変更するための新しいREST APIエンドポイントが追加されました。

- GET /api/components/{componentId}/sbom-fields
- PUT /api/components/{componentId}/sbom-fields

次のREST APIエンドポイントは、メタ/リンクセクションにsbom-fieldエンドポイントを含むコンポーネントのSBOMフィールド値を取得するように拡張されました。

- GET /api/components/{componentId}

新しいPATCH /api/settings/data-retentionエンドポイント

新しいPATCH /api/settings/data-retention REST APIエンドポイントは、既存のPUT /api/settings/data-retentionを置き換える予定です。結果として、PUT /api/settings/data-retentionは非推奨となっており、今後のリリースで削除される予定です。

新しい依存関係アップグレードガイドンスパブリックAPIエンドポイント

依存関係アップグレードガイドンスのデータを提供するための新しいREST APIエンドポイントが追加されました。

- GET /api/components/{componentId}/versions/{componentVersionId}/origins/{originId}/transitive-upgrade-guidance

/api/projects/{projectId}/versions/{projectVersionId}/matched-filesエンドポイントの更新

/api/projects/{projectId}/versions/{projectVersionId}/matched-filesエンドポイントでは、結果を表示するときの不整合の処理を改善するために、[matchTypeFilterValue]フラグが含まれるようになりました。次の表に、matchTypeがmatchTypeFilterValueにマッピングされる方法を示します。

matchType	matchTypeFilterValue
FILE_EXACT	FILES_EXACT
FILE_EXACT_FILE_MATCH	FILE_EXACT
FILE_SOME_FILES_MODIFIED	FILES_MODIFIED
FILE_DEPENDENCY_DIRECT	FILE_DEPENDENCY_DIRECT
FILE_DEPENDENCY_TRANSITIVE	FILE_DEPENDENCY_TRANSITIVE
FILE_FILES_ADDED_DELETED_AND_MODIFIED	FILES_ADDED_DELETED

バイナリスキャナ情報

バイナリスキャナがバージョン2022.9.1に更新されました。バイナリスキャナは、パッケージマネージャサポートを通じてNPMをサポートするようになりました。

2022.10.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (HUB-29825)。[システム設定] ([プロジェクトマネージャのロール設定] > [セキュリティマネージャ]) が無効になっている場合、個人のロールとグループ全体のロールの両方にグローバルセキュリティマネージャを割り当てても修復が許可されない (グレー表示になる) 問題が修正されました。
- ・ (HUB-30488)。階層型の構成表ツリーに子コンポーネントが断続的に表示されない問題を修正しました (ツリーがトリクルダウしない)。
- ・ (HUB-33274)。「構成表コンポーネント表現」に「componentVersionName」と「componentVersion」が含まれるようにREST APIドキュメントを更新しました。
- ・ (HUB-33407)。一部のユーザーが無制限のコードベースサイズを持っているときに「スキャンできるコードの最大量を超えました」という通知を受信する問題を修正しました。
- ・ (HUB-33693)。スニペットビューにアップロードされたソースウィンドウがすぐに表示されない問題を修正しました。
- ・ (HUB-33847)。プロジェクト作成リクエストの本文にクローンカテゴリフィールドcloneCategoriesが表示されない場合、すべてのクローンカテゴリが選択され、有効になる問題を修正しました。また、APIを使用してプロジェクトを作成する際に、フィールドprojectLevelAdjustmentsは、それが存在しない場合、デフォルトで「true」になります。
- ・ (HUB-33922)。[管理] > [診断] > [ジョブ] に30日分のジョブ履歴が表示されるべき場合でも、7日分のジョブ履歴だけが表示されていた問題を修正しました。
- ・ (HUB-33945、HUB-34938)。プロジェクトのBlack Duckで大規模なHTML脆弱性レポートを生成する際に、アプリケーションがクラッシュしたり、予想以上に時間がかかったりする問題を修正しました。修正の一環として、HTMLレポートのダウンロードを管理するために、設定可能なHUB_MAX_HTML_REPORT_SIZE_KBプロパティが追加されました。このプロパティはHTMLレポートの表示にのみ影響し、他のレポートの生成やダウンロードには影響しません。
- ・ (HUB-33972)。OnPrem KB Marchデータで文字列検索や著作権検索が機能しない場合がある問題を修正しました。

- ・ (HUB-34085)。コンポーネント管理ページで名前順に並べ替えると大文字と小文字が区別されていた問題を修正しました。
- ・ (HUB-34246)。[プロジェクト バージョン比較]ビューに関連するブラウザ表示の問題を修正しました。
- ・ (HUB-34511)。依存関係スキャンのプロジェクト名が中国語を使用すると読み取り不能な文字になる問題を修正しました。
- ・ (HUB-34676)。無効なカスタムフィールドを更新すると、すべてのプロジェクトバージョンで構成表の計算がトリガーされる問題を修正しました。
- ・ (HUB-34712)。BDBAコンテナのヘルスチェックのタイムアウト設定がDocker SwarmおよびKubernetesと同期していないために(30秒)、バイナリスキャンポッドがCrashLoopBackOff状態になる可能性がある問題を修正しました。また、ヘルスチェックのタイムアウト値がカスタマイズできるようになりました。
 - ・ Kubernetesの場合は、次の引数を使用します。この場合、###は秒単位です:
--set binaryscanner.timeout=###
 - ・ Docker Swarmの場合は、dockerスタック展開コマンドでタイムアウト値を指定します。この場合、###は秒単位です:

```
BDBA_HEALTH_CHECK_TIMEOUT=### docker stack deploy -c docker-compose.yml -c sizes-gen03/10sph.yaml -c docker-compose.bdba.yml hub
```
- ・ (HUB-34839)。postgres-upgraderセクションをdocker-compose.local-overrides.ymlに追加しました。
- ・ (HUB-34887)。エアギャップ環境で、自動呼び出しが長時間ハングし、登録サービスが応答しない場合にシステムが誤動作する原因となっていた問題を修正しました。
- ・ (HUB-35110)。マップされていないコードの場所のデフォルトの保持期間について、blackduck-config.env内部のドキュメントを修正しました。
- ・ (HUB-35140)。脆弱性コメントを共有しているコンポーネントのコメントが取得元固有ではない問題を修正しました。
- ・ (HUB-35184)。Black Duck 2022.4.2で見つかった脆弱性を修正するため、Zulu Javaバージョンを11.0.16+8にアップグレードしました。
- ・ (HUB-35196)。コンポーネント/コンポーネントバージョンフィルタを使用してもコンポーネント名の結果が表示されなかった問題が修正されました。
- ・ (HUB-35222)。[影響を受けるプロジェクト]タブで、特定の脆弱性(CVE-2016-1000027)のページをナビゲートするときにページをロードできなかった問題が修正されました。
- ・ (HUB-35366)。[コンポーネントの詳細]画面にカスタムフィールド値が表示されない問題を修正しました。
- ・ (HUB-35369)。Black Duck BOM pdfを印刷する場合、レポートがページの端で重なるため、すべてのコンポーネントが正しくリストされない問題を修正しました。
- ・ (HUB-35407)。null値を持つカスタムフィールドが原因でKbUpdateWorkflowJob-Component Version Updateジョブが失敗する可能性があった問題が修正されました。
- ・ (HUB-35524)。/api/projects/<project_id>/versions/<version_id>/policy-rulesパブリックエンドポイントの使用時に発生するユーザー権限の問題を修正しました。
- ・ (HUB-35660)。スキャンクライアントでエントリIDが重複しているため、終了コード70「java.util.ConcurrentModificationException」エラーが発生する可能性がある問題を修正しました。

Black Duck 2022.7.x

バージョン2022.7.2の発表

Black Duck 2022.7.2に関する新たな発表はありません。

バージョン2022.7.2の新機能および変更された機能

Black Duck 2022.7.2には、新機能や変更された機能はありません。

コンテナバージョン

- blackducksoftware/blackduck-postgres:11-2.15
- blackducksoftware/blackduck-authentication:2022.7.2
- blackducksoftware/blackduck-webapp:2022.7.2
- blackducksoftware/blackduck-scan:2022.7.2
- blackducksoftware/blackduck-jobrunner:2022.7.2
- blackducksoftware/blackduck-cfssl:1.0.9
- blackducksoftware/blackduck-logstash:1.0.20
- blackducksoftware/blackduck-registration:2022.7.2
- blackducksoftware/blackduck-nginx:2.0.25
- blackducksoftware/blackduck-documentation:2022.7.2
- blackducksoftware/blackduck-upload-cache:1.0.27
- blackducksoftware/blackduck-redis:2022.7.2
- blackducksoftware/blackduck-bomengine:2022.7.2
- blackducksoftware/blackduck-matchengine:2022.7.2
- blackducksoftware/blackduck-webui:2022.7.2
- sigsynopsys/bdba-worker:2022.6.0
- blackducksoftware/rabbitmq:1.2.10

APIの機能強化

Black Duck 2022.7.2には、新規のまたは変更されたAPIリクエストはありません。APIリクエストの詳細については、Black Duckで入手可能なREST API開発者ガイドを参照してください。

2022.7.2で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-35687)。CVEとBDSAの脆弱性が関連している場合に、関連する脆弱性が脆弱性修正に誤って追加される可能性があった問題が修正されました。この問題が発生する場合、vulnerable-bom-components APIは、この問題のあるコンポーネントに適用されるとHTTP Response 400 / Bad Requestエラーを返します。

バージョン2022.7.1の発表

Black Duck 2022.7.1に関する新たな発表はありません。

バージョン2022.7.1の新機能および変更された機能

GitリポジトリSCM統合 - フェーズ2

Black Duck 2022.7.1では、プロジェクトとバージョンの作成時にユーザーがリポジトリまたはブランチ フィールドを追加できるようになりました。承認されたSCMプロバイダ (GitHub StandardおよびGitHub Enterpriseのみ)を追加できるようになりました。この機能は、新しいプロジェクトを作成するときに選択できます。これを実行すると、新しいプロジェクトの[プロジェクト設定]ページにリポジトリURLとブランチバージョンが自動的に入力されます。

この機能はDetect 8.x以降と互換性があり、新しいスキャンで有効になります。

SCM統合はBlack Duckではデフォルトでは有効になっておらず、環境に以下を追加して有効にする必要があります。

Swarmユーザーの場合は、blackduck-config.envファイルに以下を追加します。

```
blackduck.scan.scm.enableIntegration=true
```

Kubernetesユーザーの場合は、enviromsセクションでvalues.yamlファイルに以下を追加します。

```
enviroms:
  blackduck.scan.scm.enableIntegration: "true"
```

新しいヒートマップデータのダウンロード

システム内の端末スキャンの情報を保持するヒートマップデータをダウンロードできるようになりました。この情報をダウンロードするには、[管理] > [診断] > [システム情報]の順に移動します。移動先で、[ヒートマップのダウンロード (.zip)]ボタンをクリックします。出力は.csvファイルです。

構成表にUTF8を使用したレポートの作成

この機能はBlack Duck 2022.7.0で追加されましたが、同バージョンのリリースノートから誤って省略されていることに注意してください。

Black Duck 2022.7.0では、アルファベット以外の文字を使用しているお客様向けのレポートで、構成表の文字エンコードにUTF8のサポートが導入されました。この機能を有効にするには、blackduck-config.envファイルに以下を追加します。

```
USE_CSV_BOM=true
```

プロジェクトバージョンコンポーネントでの新しい一括アクション

一括更新機能では、プロジェクトバージョンページのコンポーネントで次のアクションがサポートされるようになりました。

- ・ コンポーネントを無視/無視解除する
- ・ コンポーネントの使用法の種類を設定する
- ・ 通知ファイルに包含/除外を設定する

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:11-2.16
- ・ blackducksoftware/blackduck-authentication:2022.7.1
- ・ blackducksoftware/blackduck-webapp:2022.7.1
- ・ blackducksoftware/blackduck-scan:2022.7.1
- ・ blackducksoftware/blackduck-jobrunner:2022.7.1

- `blackducksoftware/blackduck-cfssl:1.0.9`
- `blackducksoftware/blackduck-logstash:1.0.20`
- `blackducksoftware/blackduck-registration:2022.7.1`
- `blackducksoftware/blackduck-nginx:2.0.27`
- `blackducksoftware/blackduck-documentation:2022.7.1`
- `blackducksoftware/blackduck-upload-cache:1.0.28`
- `blackducksoftware/blackduck-redis:2022.7.1`
- `blackducksoftware/blackduck-bomengine:2022.7.1`
- `blackducksoftware/blackduck-matchengine:2022.7.1`
- `blackducksoftware/blackduck-webui:2022.7.1`
- `sigsynopsys/bdba-worker:2022.6.0`
- `blackducksoftware/rabbitmq:1.2.13`

APIの機能強化

新規または変更されたAPIリクエストの詳細については、Black Duckで入手可能なAPIドキュメントを参照してください。

新しいスキャン監視APIエンドポイント

新しいREST APIエンドポイントが追加されました。このエンドポイントを使用してスキャンのエラー率を分析し、指定された時間内にシステムの端末スキャンからスキャン監視情報を取得できます（デフォルトは過去1時間に設定されています）。

- `GET /api/scan-monitor`

リクエストパラメータは次のとおりです。

- `level`（必須）。数値は1または2または3です（デフォルトは「1」）。
リクエストの例: `GET /api/scan-monitor?level=1`

失敗率が設定された最大しきい値を超えた場合（デフォルトは30%）、レベル1はOKまたはNOT OKの単純なバイナリ応答です。

レベル2は、ステータスに応じて16進数のカラーコード（緑、黄、赤）を返します。緑色（#00FF00）は、監視対象の時間内（デフォルトは過去1時間）の障害発生率が、設定されている最小しきい値（デフォルトは10%）を下回っていることを示します。黄色（#FFFF00）は、障害率が最小しきい値と最大しきい値の間（10%～30%）であることを示します。赤色（#FF0000）は、障害率が最大しきい値（30%）を超えていることを示します。

レベル3は、スキャンの状態に基づいて集計されたスキャン数を返します。

監視対象期限、最小、および最大しきい値は、ご利用されている環境の`blackduck-config.env`ファイル内で全て設定できます。

カスタムフィールドのnull値の処理の向上

次のパブリックAPIリクエストは、カスタムフィールド値がnullの場合にエラーメッセージを返すよう更新されました。

- `PUT /api/projects/{projectId}/custom-fields/{customFieldId}`
- `PUT /api/projects/{projectId}/versions/{projectVersionId}/custom-fields/{customFieldId}`
- `PUT /api/components/{componentId}/custom-fields/{customFieldId}`

- PUT /api/components/{componentId}/versions/{componentVersionId}/custom-fields/{customFieldId}
- PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/custom-fields
- PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/custom-fields/{customFieldId}
- PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/custom-fields
- PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/custom-fields/{customFieldId}

2022.7.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-33693)。パネルがクリックされない限り、スニペットを含むファイルのスキャンされたファイルビューが読み込まれなかった問題が修正されました。
- (HUB-34246)。**[プロジェクトバージョン比較]**ビューの印刷時に発生するブラウザ表示の問題が修正されました。
- (HUB-34472、HUB-34781、HUB-34682)。コンポーネントバージョンページでライセンスを削除しても構成表レポートに反映されなかった問題が修正されました。
- (HUB-34511)。プロジェクト名とバージョン名がBDIOヘッダーではなくHTTPヘッダーからプルされていたことで、ラテン文字以外の文字を使用すると読み取り不能な文字が表示されていた問題が修正されました。
- (HUB-34618)。KBオンプレミス環境でバージョン詳細レポートを生成する場合のパフォーマンスが改善されました。
- (HUB-35110)。マップされていないコードの場所のデフォルトの保持期間について、blackduck-config.env内部のドキュメントを修正しました。
- (HUB-35196)。コンポーネント/コンポーネントバージョンフィルタを使用してもコンポーネント名の結果が表示されなかった問題が修正されました。
- (HUB-35222)。**[影響を受けるプロジェクト]**タブで、特定の脆弱性(CVE-2016-1000027)のページをナビゲートするときにページをロードできなかった問題が修正されました。
- (HUB-35304)。2022.7.0へのアップグレード時に、ユーザーグループに割り当てられたスーパーユーザーの役割が2022.7.0で導入された新しい役割に移行されなかった問題が修正されました。
- (HUB-35349)。マッチングプロセスの完了後にメッセージが送信されるため、Black Duck 2022.7.0にアップグレードすると高速スキャンが失敗する可能性があった問題が修正されました。この問題は、環境で複数のマッチコンテナが実行されている場合に発生する可能性が高くなっていました。
- (HUB-35407)。null値を持つカスタムフィールドが原因でKbUpdateWorkflowJob-Component Version Updateジョブが失敗する可能性があった問題が修正されました。

バージョン2022.7.0の発表

PostgreSQL 9.6の廃止

以前に発表したとおり、PostgreSQL 9.6でのBlack Duckの実行のサポートは、Black Duckの2021.6.0リリースで終了しました。Black Duckの2022.7.0リリース以降、PostgreSQL 9.6でBlack Duckを実行しようとするとエラーが発生し、Black Duckは起動しません。

今後のPostgreSQL 11の廃止

PostgreSQL 11でのBlack Duck実行サポートは、2022.10.0リリースをもって終了します。このリリース以降、PostgreSQL 11でBlack Duckを実行しようとするとエラーが発生し、Black Duckは起動しません。

PostgreSQLコンテナの11から13への移行

Black Duck は、2022.10.0リリースでPostgreSQLイメージをバージョン11からバージョン13に移行します。Black DuckのPostgreSQLイメージを使用していないお客様には影響はありません。

今後のカスタムフィールドAPIの変更

Black Duckの2023.1.0リリースでは、無効になっているカスタムフィールドを読み取りまたは変更しようとすると、次のAPIがエラーを返すように変更されます。フィールドにアクセスするには、フィールドを再度有効にする必要があります。

- GET api/components/{componentId}/custom-fields/{custom-field-id}
- PUT api/components/{componentId}/custom-fields/{custom-field-id}
- GET api/components/{componentId}/versions/{componentVersionId}/custom-fields/{custom-field-id}
- PUT api/components/{componentId}/versions/{componentVersionId}/custom-fields/{custom-field-id}

従来の署名スキャンと従来のパッケージマネージャスキャンのサポートの廃止

この機能は、Black Duck 2023.7.0リリースで正式に廃止されます。

互換性を確保するためには、Detect 8.xにアップグレードする必要があります。Detect 8.xは、2022年5月または6月のリリースを予定していて、これはBlack Duck 2022.7.0のリリースおよびこの廃止に関するリリース ノートと一致します。これにより、将来の廃止日までDetectをアップグレードする期間として1年間の猶予が与えられます。

今後のHelm2のサポート終了

2023.1.0リリース以降、Black DuckはKubernetes導入用のHelm2をサポートしなくなります。サポートされるKubernetesの最小バージョンは1.13(Helm3でサポートされる最も古いバージョン)に引き上げられます。

訂正: GitリポジトリSCM統合 - フェーズ1

2022.4.0リリース ノートに記載されている、Swarmユーザー向けのBlack DuckでのGitリポジトリSCM統合の有効化に関する手順が正しくありませんでした。正しい変数の設定は次のとおりです。

docker-compose.yaml環境の場合:

```
webapp:
  environment:
    blackduck.scan.scm.enableIntegration: 'true'
```

また、blackduck-config.envファイルに以下を追加します。

```
blackduck.scan.scm.enableIntegration=true
```

PostgreSQLサポートスケジュールの更新

今後の2022.10.0リリース以降、Black Duckは外部PostgreSQL 11のサポートを終了します。今後のPostgreSQLバージョンに関しては、サポートの開始日と終了日を以下の表で確認してください。

PGバージョン	最初のリリース	最終リリース	BD外部サポートの追加	BD外部サポートの終了
---------	---------	--------	-------------	-------------

16.x	2023年後半	2028年後半	2024.7.0	2026.10.0
15.x	2022年後半	2027年後半	2023.7.0	2025.10.0
14.x	2021年9月	2026年11月	2022.7.0	2024.10.0
13.x	2020年9月	2025年11月	2021.8.0	2023.10.0
12.x	2019年10月	2024年11月	X	X
11.x	2018年10月	2023年11月	2020.6.0	2022.10.0

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2022.4.0が日本語にローカライズされました。

簡体字中国語


UI、オンラインヘルプ、およびリリースノートのバージョン2022.4.0が簡体字中国語にローカライズされました。

バージョン2022.7.0の新機能および変更された機能

外部データベースでのPostgreSQL 14のサポート

Black Duck は、外部PostgreSQLを使用する新規インストール用にPostgreSQL 14をサポート・推奨するようになりました。Black Duck 2022.7.xへの移行では、PostgreSQL 14への移行は不要です。

内部PostgreSQLコンテナのユーザーは、アクションは必要ありません。

 注：PostgreSQL 14.0から14.3には、インデックスが破損するというバグがあるため、サポートされているPostgreSQL 14の最小バージョンは14.4です。

スーパーユーザーの役割を管理ドメインの役割に分割

現在、スーパー ユーザーのロールを持つすべてのBlack Duckユーザーは、すべてのユーザーの権限を作成/修正でき、自分のユーザーを含む任意のユーザーにシステム管理者のロールを割り当てることができます。これにより、すべてのスーパー ユーザーが、SysAdminのロールを含む、Black Duckインスタンスへの完全なアクセスと制御を取得できるようになります。これは特権昇格の欠陥として表示されますが、役割は意図したとおりに機能しています。

このシナリオを回避するために、スーパーユーザーの役割が削除され、以前にその役割に関連付けられていたさまざまな責任を担当する次の新しい役割が作成されました：グローバルプロジェクト管理者、グローバルプロジェクトグループ管理者、ユーザー管理者、カスタムフィールド管理者。これらの新しいロールの詳細については、Black Duckヘルプを参照してください。

新しいInfrastructure as Code (IaC) の問題の表示

アプリケーションは単なるアプリケーションコードではありません。インフラストラクチャと導入方法は、アプリケーションのセキュリティを確保するための重要なコンポーネントです。そのため、IaCは、さまざまなクラウドおよびオンプレミス環境でアプリケーションの導入とセットアップを自動化するために使用されています。これらの構成オプションは、アプリケーションのセキュリティを確保する上で重要な役割を果たし、コンテナ化されたアプリケーションやサーバーベースのアプリケーションでは特に重要です。

Black Duck 2022.7.0では、スキャンにIaCが含まれている場合、プロジェクトのバージョン ページの構成表を表示するときにIaCの問題が表示されるようになりました。表示される情報は、コードで見つかった潜在的な問題に対処するのに必要な情報を提供します。

IaCスキャンを実行するには、次の[オペレーティングシステム要件](#)を満たし、Detect 7.14以降を使用している必要があります。

Infrastructure as Codeスキャンの詳細については、[コミュニティページ](#)を参照してください。

スキャンCLIの堅牢性の向上

再試行メカニズムの導入により、スキャンCLIがサーバー上で完了したときにハングしないようになりました。これは、Hub、scan、またはnginxサービスの再起動後でも、スキャンが完了し、通常どおりアップロードされることを意味します。

プロジェクトバージョンコンポーネントの一括コメントの新しいサポート

この新機能では、一括コメントを追加して、構成表のユーザーレビューとキュレーションを容易にすることができます。たとえば、コンポーネントに個別にコメントを適用する代わりに、プロジェクトバージョンページで任意の数のコンポーネントを選択し、選択したアイテムに同時にコメントを追加できます。

新しいAPIアクセストークン自動パージ機能

この新機能により、Black Duckシステムのユーザー管理者は、非アクティブなアクセストークンを自動でパージするスケジュールを設定することで、アクセストークンを介したBlack Duckへのアクセスをより適切に維持・制御できるようになります。この機能は、新しい[管理] > [アクセストークン]ページにあります。このページから、既存のすべてのアクセストークンを手動でキュレートすることもできます。

バイナリスキャンコンテナのメモリ割り当ての増加

バイナリスキャンが失敗しないように、バイナリスキャンコンテナのメモリを2 GBから4 GBに増やしました。

ポリシールールのユーザーエクスペリエンスの強化

ポリシーを作成または編集するときに、「in」または「not in」演算子が使用されている場合、コンポーネントバージョンをポリシーに追加または除外する方法を明確に示す指示が[コンポーネントの条件]に表示されるようになりました。

Black Duck KnowledgeBase検索の更新

[検索] > [Black Duck KnowledgeBase]ページの外観と、検索実行後の結果の表示方法が若干変更されました。

以前のリリースでは、Black Duck KnowledgeBase検索では、結果セットにBlack Duckプロジェクトとカスタム コンポーネントがナレッジベース コンポーネントとともに表示されました。2022.7.0以降、Black Duck KnowledgeBase検索では、ナレッジベース コンポーネント データのみが返されます。カスタムコンポーネントを検索するには、[コンポーネント検索]タブを使用する必要があります。Black Duckプロジェクトを検索するには、[プロジェクト]検索タブを使用する必要があります。

また、[Black Duck KnowledgeBase]ページの[コンポーネント ソース]フィルタ(カスタム コンポーネントおよびBlack Duckプロジェクト)が削除されました。

ナレッジベース更新ジョブのタスクの強化

以前は、ナレッジベース更新ジョブを構成するタスク(コンポーネント、コンポーネントバージョン、ライセンス、NVD脆弱性、およびBDSA脆弱性)は、事前に設定された順序で実行されていました。コンポーネントタスクが失敗した場合、後続のタスクは実行されませんでした。2022.7.0の新機能として、失敗したタスクを管理する継続メカニズムが導入されました。これにより、後続のタスクの実行がブロックされなくなります。

また、特定のタスクが失敗した理由に関する詳細情報が存在する場合は、ジョブページでより詳細に確認できます。

高速スキャンに追加された新しいプロパティ

高速スキャンの出力に、次のプロパティが追加されました。

- ・ cwelds: このセキュリティ脆弱性の共通脆弱性タイプ一覧(CWE)IDのリスト。

- ・ `shortTermUpgradeGuidance`: この脆弱性に対処するための短期的な処置として推奨されるアップグレード先のコンポーネントバージョン。これは、使用中のものと同じメジャーバージョンであるためです。
- ・ `longTermUpgradeGuidance`: 長期的な処置として推奨されるアップグレード先のコンポーネントバージョン。この処置を実行するには、メジャーバージョン番号のアップグレードが必要になる場合があります、より慎重に計画する必要があります。

Detectエンドポイントに対する新しいアップグレードガイダンス情報

Detectコンポーネントのスキャン結果に次のものが追加されました。

- ・ `shortTermUpgradeGuidance`: この脆弱性に対処するための短期的な処置として推奨されるアップグレード先のコンポーネントバージョン。これは、使用中のものと同じメジャーバージョンであるためです。
- ・ `longTermUpgradeGuidance`: 長期的な処置として推奨されるアップグレード先のコンポーネントバージョン。この処置を実行するには、メジャーバージョン番号のアップグレードが必要になる場合があります、より慎重に計画する必要があります。

プロジェクトバージョンの更新されたデータ保持管理

プロジェクトバージョンのデータ保持ポリシーをより適切に管理できるようになりました。お使いの環境で自動データ削除が有効になっている場合、削除から保護する特定のプロジェクトバージョンを選択できるようになりました。これは、新規プロジェクトを作成するとき、または既存のプロジェクトバージョンを編集するときに有効にできます。プロジェクトを表示すると、自動データ削除から保護されているプロジェクトバージョンの行の末尾にロックアイコンが表示されます。

更新されたソフトウェア構成表 (SBOM) レポートタイプとエクスポート形式

プロジェクトのソフトウェア構成表レポートをCycloneDX v1.4形式でエクスポートできるようになりました。CycloneDX v1.4形式には、セキュリティ脆弱性情報が含まれています。BDSALレコードがNVDレコードとともに含まれるようになりました。

CycloneDX v1.4の詳細については、[CycloneDX v1.4リファレンスページ](#)を参照してください。

レポートの生成後に使用されたタイプをより適切に識別できるように、レポートタイプ (SPDX、CycloneDX v1.3、またはCycloneDX v1.4) もレポート名に含まれます。

また、SBOMレポートを生成するときに、新しいレポート形式を使用できます。レポートの出力として、JSON、YAML、RDF、またはtag:valueを選択できるようになりました。

新しいデータベースパーティションジョブ

ジャーナルテーブルは月別にパーティション分割されるようになりました。最初のパーティションは特別なパーティションで、既存のすべてのジャーナルイベントが含まれています。JournalPartitionMaintenanceJobジョブは、プロジェクトの監査記録用の新しいデータベースパーティションを作成し、5年以上前の古いパーティションとジャーナルイベントを削除します。

スキャン状態/ステータスのリファクタリング

以前、スキャンステータスは、スキャン状態とスキャン進行状況の設計上の組み合わせであり、現在のキューベースのスキャンアーキテクチャではうまく機能していませんでした。新しいアプローチは、状態を提供してから、スキャンがシステム内で進行するにつれてスキャンの進行状況を追跡する方法を提供します。このアプローチは、従来のスキャンアーキテクチャを組み込んで1つのアプローチを使用できるように、十分な柔軟性を備えている必要があります。状態はデータベースに残る必要がありますが、一時的で頻繁に更新される進行状況はキャッシュに移動する必要があります。

レポートデータベースの機能強化

reporting.component_vulnerabilityマテリアライズドビューにexposed_onフィールドが追加されました。

レポートスキーマの若干の変更

2023.1.0では、255文字を超えるパスに対応できるように、reporting.scan_viewのbasedir列のタイプがcharacter varyingからtextに変更されます。

サポートされるブラウザのバージョン

- ・ Safariバージョン15.5 (17613.2.7.1.8)
 - ・ Safariバージョン13.0以前はサポートされなくなりました
- ・ Chromeバージョン103.0.5060.114 (公式ビルド) (x86_64)
 - ・ Chromeバージョン71以前はサポートされなくなりました
- ・ Firefoxバージョン102.0 (64ビット)
 - ・ Firefoxバージョン71以前はサポートされなくなりました
- ・ Microsoft Edgeバージョン103.0.1264.44 (公式ビルド) (64ビット)
 - ・ Microsoft Edgeバージョン78以前はサポートされなくなりました

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:11-2.15
- ・ blackducksoftware/blackduck-authentication:2022.7.0
- ・ blackducksoftware/blackduck-webapp:2022.7.0
- ・ blackducksoftware/blackduck-scan:2022.7.0
- ・ blackducksoftware/blackduck-jobrunner:2022.7.0
- ・ blackducksoftware/blackduck-cfssl:1.0.9
- ・ blackducksoftware/blackduck-logstash:1.0.20
- ・ blackducksoftware/blackduck-registration:2022.7.0
- ・ blackducksoftware/blackduck-nginx:2.0.25
- ・ blackducksoftware/blackduck-documentation:2022.7.0
- ・ blackducksoftware/blackduck-upload-cache:1.0.27
- ・ blackducksoftware/blackduck-redis:2022.7.0
- ・ blackducksoftware/blackduck-bomengine:2022.7.0
- ・ blackducksoftware/blackduck-matchengine:2022.7.0
- ・ blackducksoftware/blackduck-webui:2022.7.0
- ・ sigsynopsys/bdba-worker:2022.6.0
- ・ blackducksoftware/rabbitmq:1.2.10

APIの機能強化

新規または変更されたAPIリクエストの詳細については、Black Duckで入手可能なAPIドキュメントを参照してください。

Sigma Scannerをダウンロードするための新しいAPI

Sigmaバイナリをアップロードキャッシュから直接ダウンロードするための新しいエンドポイントが作成されました。API リクエストには、目的のアーキテクチャを示すのに必要なパス変数archと、versionという名前のオプションのヘッダーパラメータがあります。

```
GET /api/tools/sigma?arch={arch}
```

2022.7.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (HUB-33231)。スキャンページでスキャンサイズによってスキャンをソートしても、リストが正しい順序で表示されていなかった問題が修正されました。
- ・ (HUB-33974)。脆弱性の影響を受けるプロジェクト数が誤解を招く可能性があった問題が修正されました。コンポーネントを無視すると、[概要]ページで、特定のリスクがあるコンポーネントの数が変わります。脆弱性検索では、無視されたコンポーネントはカウントされませんが、コンポーネント検索ではカウントされます。
- ・ (HUB-32773)。コンポーネントがローカルで変更された場合に、システムがそれをKnowledgeBaseからのコンポーネントではなく、ローカル コンポーネントと見なす可能性があった問題が修正されました。構成表の計算は、コンポーネントの新しい情報を取得するときに、ナレッジベースを照会しませんでした。
- ・ (HUB-34468)。実行時間の長い他のスキャン タイプのマッチングが完了するまでの間、キューで待機しているときに、高速スキャンがタイムアウトする可能性があった問題が修正されました。
- ・ (HUB-34459)。--matchConfidenceThreshold/パラメータを従来のscan.cliで使用した場合に機能しなかった問題が修正されました。
- ・ (HUB-33477)。SAMLが無効になっている場合に、Black DuckメタデータURLダウンロード ボタンが利用可能になっていた問題が修正されました。
- ・ (HUB-33549)。[ポリシー管理] > [ポリシー ルールの作成] > [コンポーネントの条件]の[マッチ タイプ]選択リストに[直接的な依存関係バイナリ]オプションと[推移的な依存関係バイナリ]オプションがなかった問題が修正されました。
- ・ (HUB-34215)。4つの[高]の脆弱性の発見に対応して、jackson-databindおよびgsonコンポーネントを更新しました。
- ・ (HUB-33551)。コードの場所がnullのBDIOファイルをアップロードすると、ステータス コード400で失敗する可能性があった問題が修正されました。
- ・ (HUB-32919)。Hubから集約モードのBDIOを使用してスキャンをダウンロードしようとする、0バイトの破損した/空のBDIOが生成される可能性があった問題が修正されました。
- ・ (HUB-29445)。プロジェクトのREST APIフィルタリングがカンマを含むプロジェクト名をサポートしていなかった問題が修正されました。
- ・ (HUB-33164)。システム ログのサイズが大きすぎる場合に、Blackduck UIからダウンロードできなかった問題が修正されました。
- ・ (HUB-34282)。メモリの制限と予約がJavaヒープ サイズよりも512 MBを超えて大きく設定されている場合に、system_check.shスクリプトが誤警告を生成する可能性があった問題が修正されました。小さなコンテナをドキュメントに従ってセットアップした場合に誤警告が発生しないように、オーバーヘッドが20%超でメモリが1,024 MB超の場合にフラグが付けられるようにスクリプトが更新されました。
- ・ (HUB-33923)。[管理] > [診断] > [システム情報] > [ジョブ ページ]を更新した場合に、ジョブ履歴の統計情報に大幅に異なる数が表示される可能性があった問題が修正されました。
- ・ (HUB-34195)。REST APIドキュメントを更新し、[バージョン レポートの作成]セクション(または/api/versions/{projectVersionId}/reportsリクエスト)から、reportTypeからの値としてのSBOMを削除しました。

- ・ (HUB-34296)。正しくないi18n文字が原因で、日本語設定でポリシー上書き日付情報を表示できなかった問題が修正されました。
- ・ (HUB-32008)。QuartzVersionBomEventCleanupJobジョブによって「Up-to-date with error」イベントが自動クリーンアップされないことが原因で、[セキュリティ リスク ランキング]ページが処理中にスタックする可能性があった問題が修正されました。
- ・ (HUB-33727)。脆弱性の修正ステータスまたはコメントを更新する際のUIのバグを修正しました([プロジェクトバージョン]の[セキュリティ]タブ内)。
- ・ (HUB-33691)。既知の弱点がある暗号化アルゴリズムの[暗号文]タブに警告アイコンが表示されていなかったUIのバグを修正しました。
- ・ (HUB-34240)。/api/projects/{projectId}/custom-fields/{customFieldId}リクエストがnull値を送信するときに400エラーを生成する可能性があった問題が修正されました。
- ・ (HUB-34246)。[プロジェクトバージョン比較]ビューでのブラウザ表示の問題が修正されました。
- ・ (HUB-33246)。REST APIドキュメントを明確にしました。https://<server-url>/api/のhttps://.../への参照を置き換えました。
- ・ (HUB-33481)。2021.8.xとそれ以降のバージョンの間で/api/projects/{pid}/versions/{vid}/matched-files?offset=[larger than totalCount]の応答が一貫していなかった問題が修正されました。matched-filesエンドポイントは、offset>totalCountの場合でも、空のアイテムで一貫して200 OK応答を返すようになりました。
- ・ (HUB-34468)。高速スキャンが次のエラーで失敗する問題を修正しました。「開発者スキャン結果の取得中にエラーが発生しましたタイムアウトが発生した可能性があります。」または、マッチエンジンの遅延により発生するHTTP 404 Not Found応答を修正しました。
- ・ (HUB-33512)。[管理] > [設定] > [ユーザー認証]の下にある[テスト接続、ユーザー認証およびフィールド マッピング]のテキストを更新しました。「テストユーザーのメタデータのマッピング結果を表示します」という記述を削除しました。
- ・ (HUB-34836)。BLACKDUCK_HUB_SHOW_UNMATCHEDフラグが有効になっているときに、マッチしなかったコンポーネントをプロジェクト自体として編集できた問題が修正されました。
- ・ (HUB-34380)。非常に多くの調整が行われたプロジェクトで新しいバージョンをスキャンしようとしたときに、メッセージ「例外が発生しました。パラメータが多すぎます」を伴ってサーバーで新しいバージョンのBOMスキャンが失敗する可能性があった問題が修正されました。
- ・ (HUB-33793)。セキュリティ リスク ランキングの変更で「Black Duck Security Advisory」がライセンスされていない登録キーを使用した場合に、プロジェクト バージョン詳細レポートが失敗していた問題が修正されました。
- ・ (HUB-33375)。どのフィールドでソートするかを決定するループの外側にORDER_BYがあった、クエリ構築コードの不適切なSQL文法を修正しました。ソートフィールドがない場合、ORDER_BYはnullになります。
- ・ (HUB-34780)。500を超えるプロジェクト/バージョンが作成または削除された場合でも、[管理] > [診断] > [使用方法: プロジェクト] > [Project_created/Version_Created/Version_Deleted]の統計が500に制限されていた問題が修正されました。
- ・ (HUB-34592)。マッチしたコンポーネントがゼロであるが、テストで空のコンポーネントと既存のコンポーネントの両方が失敗する場合の、CodeLocationBomMatchCacheEntryエラーの逆シリアル化を修正しました。
- ・ (HUB-34588)。リンクのエンコードされていないハッシュ文字が原因で、conanパッケージの著作権リンクが機能していなかった問題が修正されました。
- ・ (HUB-24664)。BDSBackgroundUpdateWorkerが、HTTPSではなくHTTPを介して登録サーバーと通信しようとしていた問題が修正されました。
- ・ (HUB-33679)。複合要素の抽出時に、MaaS対応スキャンが失敗することがあった問題が修正されました。
- ・ (HUB-34218)。「構成表コンポーネント表現」に「componentVersionName」と「componentVersion」が含まれるようにREST APIドキュメントを更新しました。

Black Duck 2022.4.x

バージョン2022.4.2の新機能および変更された機能

データベース移行スクリプトのパフォーマンスの向上

Black Duckのバージョンをアップグレードする際に使用されるデータベース移行スクリプトのパフォーマンスが向上し、インストール時間が短縮されました。

コンテナバージョン

- blackducksoftware/blackduck-postgres:11-2.11
- blackducksoftware/blackduck-authentication:2022.4.2
- blackducksoftware/blackduck-webapp:2022.4.2
- blackducksoftware/blackduck-scan:2022.4.2
- blackducksoftware/blackduck-jobrunner:2022.4.2
- blackducksoftware/blackduck-cfssl:1.0.7
- blackducksoftware/blackduck-logstash:1.0.18
- blackducksoftware/blackduck-registration:2022.4.2
- blackducksoftware/blackduck-nginx:2.0.20
- blackducksoftware/blackduck-documentation:2022.4.2
- blackducksoftware/blackduck-upload-cache:1.0.27
- blackducksoftware/blackduck-redis:2022.4.2
- blackducksoftware/blackduck-bomengine:2022.4.2
- blackducksoftware/blackduck-matchengine:2022.4.2
- blackducksoftware/blackduck-webui:2022.4.2
- sigsynopsys/bdba-worker:2022.3.0
- blackducksoftware/rabbitmq:1.2.7

APIの機能強化

新規または変更されたAPIリクエストの詳細については、Black Duckで入手可能なAPIドキュメントを参照してください。

2022.4.2で修正された問題

Black Duck 2022.4.2には、お客様から報告された修正済みの問題は含まれていません。

バージョン2022.4.1の新機能および変更された機能

関連するマッチしなかったBDSALコードを含むCVEを自動的に無視する、新しいBDSA自動修正設定

この設定を有効にすると、修正ステータスがIGNOREDに設定され、脆弱性が修正された理由を説明するメッセージが追加されて、関連するマップされていないBDSAを含む新しいCVE脆弱性が自動的に修正されます。

この新しい設定は、関連するBDSAの脆弱性を含むCVE脆弱性にのみ適用されます。CVEはコンポーネントバージョンにマッピングされているが、関連するBDSAがそのコンポーネントバージョンにマッピングされていない場合、システムはシステム設定に基づいてCVE脆弱性を自動的に修正する可能性があります。

BDSA自動修正機能は、[管理者] > [システム設定] > [BDSA自動修正]ページで有効にできます。

高速スキャンに追加された新しいプロパティ

高速スキャンの出力に、次のプロパティが追加されました。

- `cwelds`: このセキュリティ脆弱性の共通脆弱性タイプ一覧 (CWE) ID のリスト。
- `shortTermUpgradeGuidance`: この脆弱性に対処するための短期的な処置として推奨されるアップグレード先のコンポーネントバージョン。これは、使用中のものと同一メジャーバージョンであるためです。
- `longTermUpgradeGuidance`: 長期的な処置として推奨されるアップグレード先のコンポーネントバージョン。この処置を実行するには、メジャーバージョン番号のアップグレードが必要になる場合があり、より慎重に計画する必要があります。

ユーザー権限評価のパフォーマンスの向上

ほとんどのAPIリクエストに対するユーザー権限評価が改善されました。これにより、ユーザーの役割や権限に関係なく、構成表の読み込みを含む、読み込み時の整合性が向上します。

Black Duckctlの更新

Black Duckctlが3.0.1に更新され、`sizes-gen03`展開サイズに対するBlack Duck 2022.4.0インストール サポートが追加されました。

コンテナバージョン

- `blackducksoftware/blackduck-postgres:11-2.11`
- `blackducksoftware/blackduck-authentication:2022.4.1`
- `blackducksoftware/blackduck-webapp:2022.4.1`
- `blackducksoftware/blackduck-scan:2022.4.1`
- `blackducksoftware/blackduck-jobrunner:2022.4.1`
- `blackducksoftware/blackduck-cfssl:1.0.7`
- `blackducksoftware/blackduck-logstash:1.0.18`
- `blackducksoftware/blackduck-registration:2022.4.1`
- `blackducksoftware/blackduck-nginx:2.0.16`
- `blackducksoftware/blackduck-documentation:2022.4.1`
- `blackducksoftware/blackduck-upload-cache:1.0.23`
- `blackducksoftware/blackduck-redis:2022.4.1`
- `blackducksoftware/blackduck-bomengine:2022.4.1`
- `blackducksoftware/blackduck-matchengine:2022.4.1`
- `blackducksoftware/blackduck-webui:2022.4.1`
- `sigsynopsys/bdba-worker:2022.3.0`
- `blackducksoftware/rabbitmq:1.2.7`

APIの機能強化

新規または変更されたAPIリクエストの詳細については、Black Duckで入手可能なAPIドキュメントを参照してください。

プロジェクトエンドポイントのパフォーマンスの向上

次のAPIプロジェクトエンドポイントはパフォーマンスが低下しており、最適化されました。

- `/api/projects/{ID}/versions/{ID}/compare/projects/{ID}/versions/{ID}/components`
- `/api/projects/{ID}/versions/{ID}/components`

2022.4.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-32395、HUB-33033)。マッチしたコンポーネントに対する変更済みの宣言されたライセンスがSPDXレポートに表示されないことがあった問題が修正されました。
- (HUB-29532)。ディストロイメージのrootfsパスがルートディレクトリではなくサブディレクトリで開始される場合に、Linuxディストロパッケージの一致が崩れていた問題が修正されました。
- (HUB-33947)。**[影響を受けるプロジェクト]**ページから**[修正ステータス]**を更新したときにセキュリティリスクが更新されなかった問題が修正されました。
- (HUB-33551)。コードの場所の名前がnullのbdioファイルをアップロードすると、リクエストがステータスコード400で失敗し、バックグラウンドで例外がスローされる問題が修正されました。
- (HUB-34065)。SPDX検証ツールで次のエラーの原因となっていたSPDX 2.2レポート形式が修正されました。
The following warning(s) were raised: [object instance has properties which are not allowed by the schema: ["packageSupplier"] for {"pointer":"/packages/0"}]
- (HUB-33616)。スキャンクライアントが誤ったIDでBDIOを生成することがあり(スキャンされたアーカイブ内にアーカイブエントリが重複している場合)、これによりbdioファイルがデータベースに保存されるときにエラーが発生する可能性があった問題が修正されました。
- (HUB-33915、HUB-33865)。スキャン アップロードAPIがスキャン データ全体をチャンクせずに1つのメッセージとしてRabbitMQに送信し、メッセージ サイズ エラーが発生していた問題を修正しました。
- (HUB-24664)。登録コンテナのログにHTTP経由の通信の試行が表示されていた問題が修正されました。
- (HUB-33579)。--matchConfidenceThreshold/パラメータを従来のscan.cliで使用した場合に機能しなかった問題が修正されました。
- (HUB-33311)。署名スキャナがエラー コード74で失敗する可能性がある問題を修正しました。このエラーを軽減するために、再試行機能が導入されました。

バージョン2022.4.0の発表

Spring Frameworkのセキュリティアドバイザリ(CVE-2022-22965)

Black Duck は、2022年3月30日に発表されたSpring Frameworkオープンソース ソフトウェアCVE-2022-22965(Black Duck KnowledgeBase™でBDSA-2022-0858として追跡)に関連して公開されたセキュリティ上の問題を認識しています。この脆弱性の詳細については、CVEの公式エントリを参照してください。<https://tanzu.vmware.com/security/cve-2022-22965>

2022年3月31日、SpringはSpring Frameworkバージョン5.3.18および5.2.20をリリースし、CVE-2022-22965で説明されている脆弱性に対処しました。

現在、Black Duckは、Black Duck SIGの製品、サービス、システムへの露出が制限されていると考えています。露出された範囲で、悪用を防止する緩和策を適用しています。すべての社内調査が完了し、その調査結果は、[コミュニティアドバイザリページ](#)の「製品ステータス」セクションに記載されています。

最後に、前述の調査はCVE-2022-22965 (Spring Framework) のみに焦点を当てており、CVE-2022-22963 (Spring Cloud Function) と混同しないようにしてください。

公開時に、Black DuckはSIG製品でCVE-2022-22963 (Black Duck Hub KnowledgeBase™でBDSA-2022-0850として追跡) への暴露を特定していません。この評価を変更する新しい詳細情報が入手可能になった場合は、CVE-2022-22963の別の勧告が公開されます。

Black Duck 2022.4.0へのアップグレード

Black Duck 2022.4.0へのアップグレードには、このバージョンで導入された移行スクリプトやその他の新しいプロセスの実行により、予想よりも時間がかかる場合があります。詳細については、以下の新機能と変更機能のセクションを参照してください。

リソースガイダンスの変更

デフォルトのリソース設定が更新され、すべてのスキャンボリュームの推奨設定が増加しました。以前のリソース設定は引き続き使用可能であり、以下に説明するように新しいディレクトリに移動しましたが、使用は推奨されません。

正確な推定スキャンスループットは、スキャンサイズ、タイプ、コンポジションによって異なることに注意してください。しかしながら、この内訳を社内テストで使用して、以下の表に情報を収集しました。

- ・ 50%フル署名スキャン
- ・ 40%フルパッケージマネージャスキャン
- ・ 10%開発者パッケージマネージャスキャン

コンテナリソースの制限

Black Duck 2022.4.0以降では、すべてのコンテナにリソース制限が設定されていますが、以前は一部のコンテナには設定されていませんでした。たとえば、以前のリソース割り当てでは、BomEngineコンテナのCPU制限が設定されていなかったため、制限のあるコンテナとは不釣り合いにCPUが使用される可能性がありました。以下の新しいサイズでは制限のないCPU使用が許可されないため、古い制限に近い新しいサイズを選択すると、スキャンスループットが低下することがあります。

ファイル編成の変更

上記の変更に加え、リソース上書きYAMLファイルの編成が変更されました。

Kubernetesの場合、Helmチャート内のリソース上書きYAMLファイルの編成が変更されました。

- ・ valuesフォルダの名前がsizes-gen01に変更されました。
- ・ 以前の4つのサイズ(S、M、L、XL)のファイル(small.yamlなど)は、新しいsizes-gen02ディレクトリに移動しました。
- ・ 新しいディレクトリ(sizes-gen03)には、次の表に示す各構成のリソース上書きファイルが含まれます。これらのファイルには、10sph.yaml、120sph.yamlなどの名前が付けられています。

Swarmの場合、Black Duckはコンテナ リソースをdocker-compose.ymlに直接は割り当てなくなりました。代わりに、リソースは別の上書きファイルで指定されます。以前のリソース割り当てでは(Black Duckバージョン2022.2.0以前)、sizes-gen02/resources.yamlに移動しました。Black Duck 2022.4.0以降では、sizes-gen03 folderで複数の割り当てが可能になります。

KubernetesとSwarmのどちらの場合も、1時間あたりの平均スキャン数で測定された負荷に基づいて、7つの割り当てがあります。予想される負荷が事前定義された割り当てのいずれにも一致しない場合は切り上げます。たとえば、1時間に100スキャンと予想される場合、sizes-gen03/120sph.yamlを選択します。

リソースガイドとコンテナの拡張性

これらの設定は、KubernetesとSwarmの両方のインストールに適用されます。

名前	スキャン/時間	Black Duck サービス	PostgreSQL	合計
10sph	10	CPU: 12コア メモリ: 30 GB	CPU: 2コア メモリ: 8 GB	CPU: 14コア メモリ: 38 GB
120sph	120	CPU: 13コア メモリ: 46 GB	CPU: 4コア メモリ: 16 GB	CPU: 17コア メモリ: 62 GB
250sph	250	CPU: 17コア メモリ: 118 GB	CPU: 6コア メモリ: 24 GB	CPU: 23コア メモリ: 142 GB
500sph	500	CPU: 28コア メモリ: 210 GB	CPU: 10コア メモリ: 40 GB	CPU: 38コア メモリ: 250 GB
1,000sph	1,000	CPU: 47コア メモリ: 411 GB	CPU: 18コア メモリ: 72 GB	CPU: 65コア メモリ: 483 GB
1,500sph	1,500	CPU: 66コア メモリ: 597 GB	CPU: 26コア メモリ: 104 GB	CPU: 92コア メモリ: 701 GB
2,000sph	2,000	CPU: 66コア メモリ: 597 GB	CPU: 34コア メモリ: 136 GB	CPU: 100コア メモリ: 733 GB

PostgreSQLの設定

PostgreSQLコンテナを使用しているお客様は、ALTER SYSTEMを使用して手動で値を設定する必要があります。shared_buffersへの変更は、次回PostgreSQLを再起動するまで有効になりません。これらの設定は、KubernetesとSwarmの両方のインストールに適用されます。

名前	スキャン/時間	PostgreSQL CPU/メモリ	shared_buffers (MB)	effective_cache_size (MB)
10sph	10	CPU: 2コア メモリ: 8 GB	2,654	3,185
120sph	120	CPU: 4コア メモリ: 16 GB	5,338	6,406
250sph	250	CPU: 6コア メモリ: 24 GB	8,018	9,622
500sph	500	CPU: 10コア メモリ: 40 GB	13,377	16,053
1,000sph	1,000	CPU: 18コア メモリ: 72 GB	24,129	28,955
1,500sph	1,500	CPU: 26コア メモリ: 104 GB	34,880	41,857
2,000sph	2,000	CPU: 34コア メモリ: 136 GB	45,600	54,720

今後のPostgreSQL 9.6の廃止

以前に発表したとおり、PostgreSQL 9.6でのBlack Duckの実行のサポートは、Black Duckの2021.6.0リリースで終了しました。Black Duckの2022.7.0リリース以降、PostgreSQL 9.6でBlack Duckを実行しようとするとエラーが発生し、Black Duckは起動しません。

RHEL 7およびCentOS 7でのDesktop Scannerのサポート終了

2022.4.0以降、Black DuckはRed Hat Enterprise Linux 7およびCentOS 7用のDesktop Scannerの新しいバージョンを構築しなくなります。また、次期2022.7.0リリースでは、バイナリはすべて削除される予定です。

PostgreSQLサポートスケジュールの更新

今後の2022.10.0リリース以降、Black Duckは外部PostgreSQL 11のサポートを終了します。今後のPostgreSQLバージョンに関しては、サポートの開始日と終了日を以下の表で確認してください。

PGバージョン	最初のリリース	最終リリース	BD外部サポートの追加	BD外部サポートの終了
16.x	2023年後半	2028年後半	2024.7.0	2026.10.0
15.x	2022年後半	2027年後半	2023.7.0	2025.10.0
14.x	2021年9月	2026年11月	2022.7.0	2024.10.0
13.x	2020年9月	2025年11月	2021.8.0	2023.10.0
12.x	2019年10月	2024年11月	X	X
11.x	2018年10月	2023年11月	2020.6.0	2022.10.0

Azure PostgreSQL 13 Flexサーバー構成

Black Duckをインストールすると、initスクリプトexternal-postgres-init.pgsqlの実行時に、Azureユーザーに次のエラーメッセージが表示されることがあります。

```
psql:/dev/fd/63:25: ERROR: extension "pgcrypto" is not allow-listed for "azure_pg_admin" users in Azure Database for PostgreSQL
```

このエラーを回避するには、Azure PG 13 Flexサーバーの使用時に、サーバーパラメーターazure.extensions[]に値PGCRYPTOがあることを確認してください。

非推奨API

次のレガシーAPI Solrエンドポイントは非推奨となり、Black Duck 2022.7.0リリースでは削除されます。

- ・ GET /api/search/components
- ・ GET /api/autocomplete/component

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2022.2.0が日本語にローカライズされました。

簡体字中国語

UI、オンラインヘルプ、およびリリースノートのバージョン2022.2.0が簡体字中国語にローカライズされました。

バージョン2022.4.0の新機能および変更された機能

Spring Frameworkの更新

Spring Frameworkは、重要なCVE-2022-22965の脆弱性に対処するために5.3.18に更新されました。

新しい脆弱性のメトリックの比較

この新機能により、脆弱性の概要ページが変更され、必要に応じてメトリックを並べて表示できるようになりました。BDSAとNVDの両方のレコードがある脆弱性を表示すると、[スコアとメトリック]セクションに、BDSAとNVDの両方の脆弱性タイプを比較したグラフが表示されます。CVSS v2とCVSS v3.xを交互に使用して、詳細を把握してください。

GitリポジトリSCM統合 - フェーズ1

Black Duck 2022.4.0では、リポジトリ、ブランチ、ビルド、リリースの管理に統合を活用することで、顧客の新規プロジェクトのオンボーディングを簡素化する方法が導入されます。フェーズ1から、プロジェクト作成モダリティおよびプロジェクト設定ページに新しいSCM URLフィールドが、プロジェクトバージョン設定ページにSCMブランチフィールドが追加されます。

このフェーズでは、これらのフィールドに手動で情報を入力します。ただし、次のDetectリリースでは、gitリポジトリのスキャン後に自動的に情報が入力されます。Detectは、関連付けられているgitリポジトリのURLとブランチを自動で識別し、その情報をBlack Duckに送信します。

この機能はBlack Duckではデフォルトでは有効になっておらず、環境に以下を追加して有効にする必要があります。

Swarmユーザーの場合は、以下をdocker-compose.yml webapp環境に追加します。

```
webapp:
  environment: {blackduck.scan.scm.enableIntegration: true}
```

Kubernetesユーザーの場合は、以下をwebappコンテナ環境に追加します。

```
containers:
- env:
  - name: blackduck.scan.scm.enableIntegration
    value: true
```

BDSA脆弱性の新しい[コンポーネント]タブ

新しい[コンポーネント]タブが、BDSA脆弱性レコードに追加されました。このタブでは、特定のBDSA脆弱性の影響を受ける既知のすべてのコンポーネントバージョンを確認できます。

コンポーネントダッシュボードの拡張によってクエリ表示を実現

SearchDashboardRefreshJobに関連するすべてのクエリは、パフォーマンスを向上させるために最適化されました。LicenseDashboardRefreshJobの使用が可能になり、それに関連するビューがSearchDashboardRefreshJobの下で更新されます。つまり、[ライセンス管理]ページに表示されるカウントが、SearchDashboardRefreshJobの終了時に更新されます。

注:これらの変更の結果、Black Duck 2022.4.0へのアップグレードには、移行スクリプトの実行のために通常より時間がかかる場合があります。

PostgreSQL 11コンテナの移行

Black Duck提供のPostgreSQLコンテナを使用したKubernetesとOpenShiftの導入において、2022.2.0で追加された次の永続ボリューム要求は不要になりました。このボリューム要求とそれに関連付けられている永続ボリュームは安全に削除できます。

```
{{ .Release.Name }}-blackduck-postgres-tmp
```

Javaヒープサイズ割り当ての更新と新しい環境変数

以前のリリースでは、JavaはヒープサイズをHUB_MAX_MEMORYにまで徐々に増加させることが許可されていました。Black Duck 2022.4.0以降では、効率性と予測可能性を活用するために、起動時にHUB_MAX_MEMORY全体が事前に割り当てられます。

この更新の一環として、次の新しい環境変数が追加されました。HUB_MIN_MEMORY.この変数を使用すると、Javaヒープサイズの下限を設定できます。

デフォルトでは最適な設定として、HUB_MIN_MEMORYはHUB_MAX_MEMORYに等しく設定されますが、512mなどの少ない量に明示的に設定し、HUB_MIN_MEMORYからHUB_MAX_MEMORYまで徐々にJavaにメモリを取得させることができます。

高速スキャンポリシーの上書きを特定の脆弱性に制限

以前のBlack Duckバージョンでは、高速スキャン ポリシー違反がポリシーとコンポーネントによって上書きされる可能性があります。ただし、新しい脆弱性が見つかった場合、既存の上書きによって違反が抑制され、偽陰性になる可能性があります。

Black Duck 2022.4.0では、既存のYAMLアップロード メカニズムを使用し、高速スキャンの特定の脆弱性を上書きできるようになりました。

脆弱性IDでは、予想される形式への一致が検証されます。

```
---
version: 1.0
policy:
  overrides:
    - policyName: policyA
      components:
        - name: component1
          version: version1
          vulnerabilities:
            - vulnerabilityId1
            - vulnerabilityId2
        - name: component2
    - policyName: policyB
      components:
        - name: component3
```

新しい高速スキャンの脆弱性プロパティの追加

高速スキャンの出力の脆弱性には、次のプロパティが追加されました。

- publishedDate(日付値)
- vendorFixDate(日付値)
- workaround(文字列値)
- solution(文字列値)


新しいBDSA自動修正設定(ベータ版)

Black Duck Security Advisory(BDSA)チームは、CVE脆弱性を分析する際に、脆弱性の影響を受けるコンポーネントバージョンを確認します。場合によっては、この脆弱性がさまざまなバージョンに適用されることがわかります。この新機能を使用すると、脆弱性がそのコンポーネントバージョンに適用されないことをBDSAチームが発見した場合に、CVE脆弱性を自動的に無視することができます。これは、ステータスがNEWの脆弱性にものみ影響します。

BDSA自動修正はベータ機能であり、デフォルトでは有効になっていません。この機能を有効にするには、次の環境変数を設定する必要があります。

```
BDSA_AUTO_REMEDIATION=true
```

BDSA自動修正設定は、[管理者] > [システム設定] > [BDSA自動修正]ページで変更できます。

 注：ユーザーが設定を保存するたびに、システムによってチェックが行われ、すべてのプロジェクトの脆弱性が更新される可能性があります。大規模なシステムではこれに時間がかかり、Black Duckのパフォーマンスに影響する可能性があります。

ユーザーとグループの管理表示を更新

[管理者] > [ユーザーとグループ]の[ユーザー]タブと[グループ]タブの外観が更新され、さまざまなセクション(ユーザー/グループの詳細、全体的な役割、プロジェクトグループ、プロジェクト、ユーザー/ユーザーグループ)がそれぞれのページに分かれて明確に表示され、ユーザーとグループの管理が容易になりました。

ポリシーの新しいコンポーネント条件ルール

未確認スニペットの新しいコンポーネント条件が追加されました。新しいポリシー条件では、ポリシーを作成または編集して、レビューされていないスニペットにポリシー違反をトリガーできます。

新しいソフトウェア構成表(SBOM)レポートのCycloneDX v1.3エクスポート形式

プロジェクトのソフトウェア構成表レポートをCycloneDX v1.3形式でエクスポートできるようになりました。これを行うには、プロジェクトバージョンを表示して[レポート]タブ[レポートの作成]ボタンの順にクリックし、CycloneDX v1.3 — JSONを選択します。CycloneDX v1.3の詳細については、「[CycloneDX v1.3リファレンスページ](#)」をご参照ください。

新しいコンポーネント依存関係の重複感度システムプロパティ

新しいシステム プロパティがBlack Duckに追加され、パッケージ マネージャ スキャンで結果の依存関係ツリーに追加するコンポーネントごとにノード(マッチ)の最大数を制御できるようになりました。

`blackduck.match.limit.per.component`

このシステムプロパティのデフォルト値は10であるため、ツリー内で重複するコンポーネントの数は、`blackduck.match.limit.per.component`の値(コンポーネントごとのマッチ制限)を超えることはできません。

サポート対象ブラウザのバージョン

- ・ Safariバージョン15.4(16613.1.17.1.13、16613)
 - ・ Safariバージョン13.0以前はサポートされなくなりました
- ・ Chromeバージョン100.0.4896.75(公式ビルド)(x86_64)
 - ・ Chromeバージョン71以前はサポートされなくなりました
- ・ Firefoxバージョン99.0(64ビット)
 - ・ Firefoxバージョン71以前はサポートされなくなりました
- ・ Microsoft Edgeバージョン100.0.1185.36(公式ビルド)(64ビット)
 - ・ Microsoft Edgeバージョン78以前はサポートされなくなりました

コンテナバージョン

- ・ `blackducksoftware/blackduck-postgres:11-2.11`
- ・ `blackducksoftware/blackduck-authentication:2022.4.0`
- ・ `blackducksoftware/blackduck-webapp:2022.4.0`
- ・ `blackducksoftware/blackduck-scan:2022.4.0`
- ・ `blackducksoftware/blackduck-jobrunner:2022.4.0`

- blackducksoftware/blackduck-cfssl:1.0.7
- blackducksoftware/blackduck-logstash:1.0.18
- blackducksoftware/blackduck-registration:2022.4.0
- blackducksoftware/blackduck-nginx:2.0.14
- blackducksoftware/blackduck-documentation:2022.4.0
- blackducksoftware/blackduck-upload-cache:1.0.23
- blackducksoftware/blackduck-redis:2022.4.0
- blackducksoftware/blackduck-bomengine:2022.4.0
- blackducksoftware/blackduck-matchengine:2022.4.0
- blackducksoftware/blackduck-webui:2022.4.0
- sigsynopsys/bdba-worker:2021.12.2
- blackducksoftware/rabbitmq:1.2.7

APIの機能強化

新規または変更されたAPIリクエストの詳細については、Black Duckで入手可能なAPIドキュメントを参照してください。

プロジェクトエンドポイントのパフォーマンスの向上

次のAPIプロジェクトエンドポイントはパフォーマンスが低下しており、最適化されました。

- /api/projects/{ID}/versions/{ID}/compare/projects/{ID}/versions/{ID}/components
- /api/projects/{ID}/versions/{ID}/components

2022.4.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-33047)。KbUpdateJobプロセス中にNULLポインタ例外エラーが発生した場合、ジョブの進行が非常に遅くなったり、スタックしているように見えたりしていた問題を修正しました。
- (HUB-32336)。BOMページの[コンポーネント]フィルタの名前は、実際の機能に合わせて[コンポーネントバージョン]に変更されました。
- (HUB-32316)。JVMの最大メモリ割り当てプールを定義するHUB_MAX_MEMORY環境変数がDocker登録コンテナ展開で設定されないままになっていた問題が修正されました。
- (HUB-32492)。MITライセンスがBlack Duckで承認済みに設定されていたとしても、MITライセンスを持つコンポーネントが高速スキャンで「ライセンス未承認」および「ライセンス未確認」のポリシー違反をトリガーする可能性があった問題が修正されました。
- (HUB-31839)。BDIOアップロードエンドポイントプロジェクトとバージョン値がURLデコードされていなかった問題が修正されました。
- (HUB-32692、HUB-32672)。コンポーネントに複数の脆弱性があり、それぞれの脆弱性ステータスが異なる場合、コンポーネントのすべての脆弱性が選択したポリシールールに一致しない限り、ポリシールールがポリシー違反をトリガーしない可能性があった問題が修正されました。
- (HUB-31872)。高速スキャンでユーザー権限が検証されていなかった問題が修正されました。一致するプロジェクトバージョンBOMがスキャンで検出されたが、ユーザーに権限がない場合、スキャンはプロジェクトバージョンまたはBOMコンポーネントデータなしで実行されます。

- ・ (HUB-33231)。スキャンページでスキャンサイズによってスキャンをソートしても、リストが正しい順序で表示されていなかった問題が修正されました。
- ・ (HUB-33096)。ライセンス ファミリによってフィルタリングしても、修正されたKnowledgeBaseライセンスが正しく表示されない可能性があった問題が修正されました。
- ・ (HUB-30463)。golang.org/x/sysコンポーネントがHub UIナレッジベース検索に表示されていなかった問題が修正されました。
- ・ (HUB-31891)。Apache HTTPサーバーコンポーネントを検索すると、Debianコンポーネントページにリンクしていた問題が修正されました。
- ・ (HUB-28406)。一部のOSSコンポーネントおよびバージョンにおいて、[セキュリティ]タブと[詳細情報]タブに表示される脆弱性の数が異なることがあった問題を修正しました。
- ・ (HUB-32883)。accessTokenValiditySeconds設定のMax-AgeおよびExpiresフィールドがJSON Webトークン (JWT) の有効期限値と一致しなかった問題が修正されました。
- ・ (HUB-32313)。パッケージマネージャのスキャンデータの高負荷を処理する際のREST API /api/projects/<id>/versions/<id>/componentsエンドポイントのパフォーマンスの問題が修正されました。
- ・ (HUB-32571)。コンポーネント バージョンの著作権タブおよびBlack Duck通知レポート(およびBOMセキュリティタブ)で、元の名前空間の表示が一貫していなかった問題が修正されました。
- ・ (HUB-32949)。ユーザーをプロジェクトグループに直接割り当て、同じユーザーをプロジェクトグループに割り当てられているユーザーグループにも割り当てると、複数のプロジェクトグループがAPIによって返されてDetectが失敗していた問題が修正されました。
- ・ (HUB-33132)。依存関係パスAPIが大量のサービスメモリを消費し、ディスクにページングしていた問題が修正されました。
- ・ (HUB-33155)。ハブ登録の更新が停止し、JobRunnerがロックを保持する時間が長引いて、クエリがブロックされていた問題が修正されました。
- ・ (HUB-32010)。プロジェクトグループ階層を移動するときに、サブグループ内のプロジェクトをクリックすると、ユーザーがルートプロジェクトグループに戻る可能性があった問題が修正されました。
- ・ (HUB-32977)。大文字と小文字が混在したタグがポリシー ルールを想定どおりにトリガーしていなかった問題が修正されました。
- ・ (HUB-33305)。docker-compose.local-overrides.ymlファイル内のインデントの問題が修正されました。
- ・ (HUB-27940)。最小CPUリソースが指定されていない状態でEKSに展開するとき、ポッドに0.25 (250m) のCPUコアが割り当てられ、bomengine/rabbitmqが動作しなかった問題が修正されました。
- ・ (HUB-33455)。CVE-2022-23395の脆弱性の詳細ページへのリンクが404 Not Foundエラーページに移動していた問題が修正されました。
- ・ (HUB-32256)。カスタム署名レベルに空の値を送信すると、誤ったエラーメッセージが生成される可能性があった問題が修正されました。
- ・ (HUB-32800)。依存関係ツリー内のコンポーネントごとに大量のマッチがあるため、bitbake/yoctoスキャン中にJobRunnerでmatchengineが再起動するかジョブがハングし、OutOfMemory例外が発生することがあった問題が修正されました。詳細については、上記の新機能および変更された機能に関するセクションの「新しいコンポーネント依存関係の重複感度システムプロパティ」を参照してください。
- ・ (HUB-33349)。webappコンテナがデフォルトで{{ .Release.Name }}-blackduck-webappという名前の永続ボリューム (Release.Nameは一般的にhubまたは展開時に選択した別のラベル) を必要としていた問題が修正されました。また、webapp values.yamlのオーバーライドでpersistentVolumeClaimNameを設定することで、カスタム永続ボリューム名を設定しているお客様もいます。これらの設定、永続ボリューム、永続ボリューム要求は不要になり、安全に削除できます。

- ・ (HUB-32678)。デフォルトのIPスキャンで、一致するコンポーネントをフィルタリングするためのscan.cli引数--matchConfidenceThresholdがサポートされていなかった問題が修正されました。
- ・ (HUB-29532)。ディストロイメージのrootfsパスがルートディレクトリではなくサブディレクトリで開始される場合に、Linuxディストロパッケージの一致が崩れていた問題が修正されました。

Black Duck 2022.2.x

バージョン2022.2.2の新機能および変更された機能

Black Duck バージョン2022.2.2はメンテナンスリリースであり、新機能や変更された機能はありません。セキュリティ脆弱性を回避するために、オンラインヘルプを修正しました。

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:11-2.8
- ・ blackducksoftware/blackduck-authentication:2022.2.2
- ・ blackducksoftware/blackduck-webapp:2022.2.2
- ・ blackducksoftware/blackduck-scan:2022.2.2
- ・ blackducksoftware/blackduck-jobrunner:2022.2.2
- ・ blackducksoftware/blackduck-cfssl:1.0.6
- ・ blackducksoftware/blackduck-logstash:1.0.16
- ・ blackducksoftware/blackduck-registration:2022.2.2
- ・ blackducksoftware/blackduck-nginx:2.0.12
- ・ blackducksoftware/blackduck-documentation:2022.2.2
- ・ blackducksoftware/blackduck-upload-cache:1.0.21
- ・ blackducksoftware/blackduck-redis:2022.2.2
- ・ blackducksoftware/blackduck-bomengine:2022.2.2
- ・ blackducksoftware/blackduck-matchengine:2022.2.2
- ・ blackducksoftware/blackduck-webui:2022.2.2
- ・ sigsynopsys/bdba-worker:2021.12.2
- ・ blackducksoftware/rabbitmq:1.2.7

APIの機能強化

新規または変更されたAPIリクエストの詳細については、Black Duckで入手可能なAPIドキュメントを参照してください。

2022.2.2で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (HUB-34065)。SPDX検証ツールで次のエラーの原因となっていたSPDX 2.2レポート形式が修正されました。
The following warning(s) were raised: [object instance has properties which are not allowed by the schema: ["packageSupplier"] for {"pointer":"/packages/0"}]

バージョン2022.2.1の新機能および変更された機能

更新されたデータ削除機能（ベータ版）

データ削除機能を使用すると、定義した条件に従ってプロジェクトバージョンを自動的に削除する方法を検討できます。バージョン制限、ディスク容量の制約、またはデータベースのボトルネックがあるユーザーの場合、古いバージョンの増加は、プロセスまたはシステムパフォーマンスのいずれかで問題となる可能性があります。この機能は、時間の経過とともに複数のプロジェクトバージョンを生成し、時間の経過とともに廃版になる場合に役立ちます。

Black Duck 2022.2.0では、以下の新しい環境変数が追加されました。

- ・ `BLACKDUCK_AUTOMATIC_VERSION_REMOVAL_RELEASE_PHASES`
 - ・ データ削除プロセスに適用できるプロジェクトバージョンフェーズを定義します。
 - ・ リリースフェーズの値は、Planning（計画）、Development（開発）、Released（リリース）、Deprecated（廃止）、Archived（アーカイブ）、Prerelease（プレリリース）です。
 - ・ 設定しない場合、デフォルト値はDevelopmentです。
 - ・ 値では大文字と小文字が区別されません。
 - ・ 複数のリリースフェーズは、カンマで区切って追加できます。

プロジェクトおよびプロジェクトグループの役割割り当てを更新

プロジェクトおよびプロジェクトグループにプロジェクトビューアとしてユーザーを追加できるようになりました。プロジェクトまたはプロジェクトグループにユーザーを追加すると、プロジェクトビューアの役割が自動的に選択され、デフォルトの役割として機能します。その後、必要に応じてユーザーに役割を追加できます。

最小スキャン間隔の設定を更新

Detect 7.13以降から、Black Duck Hubスキャン設定の最小スキャン間隔は無効になります。最小スキャン間隔は、次のようにDetectを使用してコマンド引数として設定する必要があります。

```
--detect.blackduck.signature.scanner.arguments='--min-scan-interval=##'
```

ここで、##は時間単位の時間です。

コンテナバージョン

- ・ `blackducksoftware/blackduck-postgres:11-2.8`
- ・ `blackducksoftware/blackduck-authentication:2022.2.1`
- ・ `blackducksoftware/blackduck-webapp:2022.2.1`
- ・ `blackducksoftware/blackduck-scan:2022.2.1`
- ・ `blackducksoftware/blackduck-jobrunner:2022.2.1`
- ・ `blackducksoftware/blackduck-cfssl:1.0.6`
- ・ `blackducksoftware/blackduck-logstash:1.0.16`
- ・ `blackducksoftware/blackduck-registration:2022.2.1`
- ・ `blackducksoftware/blackduck-nginx:2.0.12`
- ・ `blackducksoftware/blackduck-documentation:2022.2.1`
- ・ `blackducksoftware/blackduck-upload-cache:1.0.21`
- ・ `blackducksoftware/blackduck-redis:2022.2.1`

- [blackducksoftware/blackduck-bomengine:2022.2.1](#)
- [blackducksoftware/blackduck-matchengine:2022.2.1](#)
- [blackducksoftware/blackduck-webui:2022.2.1](#)
- [sigsynopsys/bdba-worker:2021.12.2](#)
- [blackducksoftware/rabbitmq:1.2.7](#)

APIの機能強化

新規または変更されたAPIリクエストの詳細については、Black Duckで入手可能なAPIドキュメントを参照してください。

2022.2.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-32540)。重複した値を挿入すると、ジョブの速度が低下したり、ジョブが失敗したりする可能性があるという、KbUpdateJobでまれに発生していた問題が修正されました。
- (HUB-32544)。スキャンによってすでに挿入されたversion_bom_componentをKbUpdateJobが挿入しようとする競合状態の問題が修正されました。
- (HUB-33045)。高速スキャン専用のポリシールールを作成すると、すべてのプロジェクトバージョンが再計算状態になり、BOMのステータスが「処理中」に変わる可能性があった問題が修正されました。
- (HUB-32363およびHUB-33027)。次のシナリオでコードの場所をマッピング解除している間の競合状態を修正しました(--detect.project.codelocation.unmap=trueを使用しない)。
 - コードの場所を再スキャンし、他のプロジェクトバージョンにマッピングする。
 - コードの場所をUIから手動でマッピング解除する。
 - コードの場所をUIから手動で削除する。
 - コードの場所をScanPurgeJobによって削除する。
- (HUB-33155)。ハブ登録の更新が停止し、JobRunnerがロックを保持する時間が長引いて、クエリがブロックされていた問題が修正されました。
- (HUB-33132)。依存関係パスAPIが大量のサービスメモリを消費し、ディスクにページングしていた問題が修正されました。
- (HUB-31212)。1つのサブプロジェクト グループのメンバーがすべてのプロジェクト グループとそのツリーにアクセスできる可能性があった問題を修正しました。
- (HUB-33162)。最高優先度のセキュリティ リスク ランキング セットが脆弱性タイプ(BDSAとNVD)およびCVSS プリファレンスと一致しない場合に、高速スキャンで不正確な情報が表示される可能性があった問題を修正しました。
- (HUB-31756)。プロジェクト ビューアとプロジェクト グループ ビューアのロールが、プロジェクトおよびプロジェクト グループに追加されたユーザーに割り当て可能ではなかった問題を修正しました。
- (HUB-33047)。KbUpdateJobプロセス中にNULLポインタ例外エラーが発生した場合、ジョブの進行が非常に遅くなったり、スタックしているように見えたりしていた問題を修正しました。

バージョン2022.2.0の発表

強化された署名生成

Black Duck 2022.2.0以降、署名スキャナはデフォルトでは、サーバーではなくクライアント上で署名を生成するようになります。

Black Duckでホストされるサービスを使用している場合、またはこのリリースに含まれているHelmチャートまたはDocker Swarm 'yaml'ファイルを使用している場合、この変更はシームレスに行われ、ユーザー側での操作は必要ありません。サービスの中断はありません。

ただし、Helmチャートをカスタマイズした場合や、上書きファイルを使用する場合は、移行に役立つ追加情報について、コミュニティページの「[再バランシングのガイダンス](#)」を参照してください。

APIリクエストのページ数制限の最大値

システムリソースの管理を改善する継続的な取り組みで、最大ページ数の制限が特定のAPIリクエストに導入されました。最大ページ数制限は1000ページに設定されますが、Black Duckの今後のバージョンで変更される可能性があります。2022.2.0バージョンで影響を受けるAPIリクエストのリストについては、以下の「APIの機能強化」セクションを参照してください。

廃止されたAPI

Black Duck 2022.2.0では、`/cpes/{cpeId}/variants`エンドポイントが廃止され、`/cpes/{cpeId}/origins`に置き換えられます。`/cpes/{cpeId}/variants`は、Black Duck 2022.4.0で削除されます。`/api/cpes`のメタデータ内のAPIリンクも、`/api/cpes/{cpeId}/variants`ではなく、`/api/cpes/{cpeId}/origins`を返すように更新されています。

今後のリソースガイダンスの変更

Black Duck 2022.4.0リリースでは、デフォルトのリソース設定が更新され、すべてのスキャン ボリュームの推奨設定が増加します。2022.4.0リリースには、既存の設定を引き続き使用する方法についての説明が付属しています。

正確な推定スキャンスループットは、スキャンサイズ、タイプ、コンポジションによって異なることに注意してください。しかしながら、この内訳を社内テストで使用して、以下の表に情報を収集しました。

- ・ 50%フル署名スキャン
- ・ 40%フルパッケージマネージャスキャン
- ・ 10%開発者パッケージマネージャスキャン

ファイル編成の変更

2022.4.0以降では、上記の変更に加え、リソース上書きYAMLファイルの編成が変更されます。

Kubernetesの場合、Helmチャート内のリソース上書きYAMLファイルの編成が変更されます。

- ・ `values`フォルダの名前が`sizes-gen01`に変更されます。
- ・ 以前の4つのサイズ(S、M、L、XL)のファイル(`small.yaml`など)は、新しい`sizes-gen02`ディレクトリに移動します。
- ・ 新しいディレクトリ(`sizes-gen03`)には、次の表に示す各構成のリソース上書きファイルが含まれます。これらのファイルには、`10sph.yaml`、`120sph.yaml`などの名前が付けられています。

Swarmの場合、Black Duckはコンテナ リソースを`docker-compose.yml`に直接は割り当てなくなります。代わりに、リソースは別の上書きファイルで指定されます。現在のリソース割り当ては`sizes-gen02/resources.yaml`に移動されます。Black Duck 2022.4.0以降では、`sizes-gen03` folderで複数の割り当てが可能になります。

KubernetesとSwarmのどちらの場合も、1時間あたりの平均スキャン数で測定された負荷に基づいて、7つの割り当てがあります。予想される負荷が事前定義された割り当てのいずれにも一致しない場合は切り上げます。たとえば、1時間に100スキャンと予想される場合、`sizes-gen03/120sph.yaml`を選択します。

リソースガイドとコンテナの拡張性

これらの設定は、KubernetesとSwarmの両方のインストールに適用されます。

名前	スキャン/時間	Black Duck サービス	PostgreSQL	合計
10sph	10	CPU: 10コア メモリ: 29 GB	CPU: 2コア メモリ: 8 GB	CPU: 12コア メモリ: 37 GB
120sph	120	CPU: 12コア メモリ: 46 GB	CPU: 4コア メモリ: 16 GB	CPU: 16コア メモリ: 62 GB
250sph	250	CPU: 16コア メモリ: 106 GB	CPU: 6コア メモリ: 24 GB	CPU: 22コア メモリ: 131 GB
500sph	500	CPU: 27コア メモリ: 208 GB	CPU: 10コア メモリ: 40 GB	CPU: 37コア メモリ: 249 GB
1,000sph	1,000	CPU: 47コア メモリ: 408 GB	CPU: 18コア メモリ: 72 GB	CPU: 65コア メモリ: 480 GB
1,500sph	1,500	CPU: 66コア メモリ: 593 GB	CPU: 26コア メモリ: 104 GB	CPU: 92コア メモリ: 697 GB
2,000sph	2,000	CPU: 66コア メモリ: 593 GB	CPU: 34コア メモリ: 136 GB	CPU: 100コア メモリ: 729 GB

PostgreSQLの設定

PostgreSQLコンテナを使用しているお客様は、ALTER SYSTEMを使用して手動で値を設定する必要があり、`shared_buffers`への変更は、次回PostgreSQLを再起動するまで有効になりません。これらの設定は、KubernetesとSwarmの両方のインストールに適用されます。

名前	スキャン/時間	PostgreSQL CPU/メモリ	<code>shared_buffers</code> (MB)	<code>effective_cache_size</code> (MB)
10sph	10	CPU: 2コア メモリ: 8 GB	2,654	3,185
120sph	120	CPU: 4コア メモリ: 16 GB	5,338	6,406
250sph	250	CPU: 6コア メモリ: 24 GB	8,018	9,622
500sph	500	CPU: 10コア メモリ: 40 GB	13,377	16,053
1,000sph	1,000	CPU: 18コア メモリ: 72 GB	24,129	28,955
1,500sph	1,500	CPU: 26コア メモリ: 104 GB	34,880	41,857
2,000sph	2,000	CPU: 34コア メモリ: 136 GB	45,600	54,720

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.10.0が日本語にローカライズされました。

簡体字中国語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.10.0が簡体字中国語にローカライズされました。

バージョン2022.2.0の新機能および変更された機能

Logstashの更新

[CVE-2021-44832](#)の脆弱性に対処するため、Black Duckで使用されるLogstashイメージは、Log4j2バージョン2.17.1を使用する7.16.3にアップグレードされました。

強化された署名生成

「発表」で述べたように、署名スキャナはデフォルトでは、サーバーではなくクライアント上で署名を生成するようになります。

Black Duckでホストされるサービスを使用している場合、またはこのリリースに含まれているHelmチャートまたはDocker Swarm 'yaml'ファイルを使用している場合、この変更はシームレスに行われ、手動の操作は必要ありません。サービスの中断はありません。

ただし、Helmチャートをカスタマイズした場合や、上書きファイルを使用する場合は、移行に役立つ追加情報について、コミュニティの「[再バランシングのガイダンス](#)」の記事を参照してください。

コミュニティでは、[PrometheusとGrafanaを使用したBlack Duckの監視](#)に関する詳細も記載されています。

高速スキャンの機能強化

同じエンドポイントが使用されますが、高速スキャンモードを受け入れるために新しいヘッダーが追加されました。新しいHTTPヘッダーは「X-BD-RAPID-SCAN-MODE」という名前であり、次の値を受け入れます。

- ALL: デフォルトの操作。RAPIDまたは(RAPIDおよびFULL)であるポリシールールを評価します。ヘッダーがnullの場合は、これがデフォルトになります。
- BOM_COMPARE: ALLなどのすべてのポリシールールを評価しますが、ポリシールールモードのタイプに基づいて別々に評価を行います。ポリシールールが(RAPIDおよびFULL)の場合は、BOM_COMPARE_STRICTと同様に動作しますが、ポリシールールが(RAPID)のみである場合は、ALLと同様に動作します。RAPIDのみのポリシーは、結果にnullのポリシーステータスが表示されます。
- BOM_COMPARE_STRICT: (RAPIDおよびFULL)であるポリシールールのみを評価します。陽性結果に含まれるすべてのポリシールールのステータスは、NEWまたはRESOLVEDになります。ポリシー違反は、既存のプロジェクトバージョンの構成表と比較されます。ポリシー違反が既知で、すでに構成表に表示されていた場合(アクティブまたは上書き)、そのポリシー違反は高速スキャンの陽性結果には含まれませんが、既存の制限に従った完全な結果には含まれます。

BOM_COMPAREモードのいずれかを実行するには、HUBに既存のプロジェクトバージョンが必要です。

PostgreSQL 11コンテナの移行

CentOS PostgreSQL 9.6コンテナは、Black Duck PostgreSQL 11コンテナに置き換えられました。新しいblackduck-postgres-upgraderコンテナは、PostgreSQL 9.6からPostgreSQL 11にデータベースを移行し、完了すると終了します。

コア以外のPG拡張機能を使用しているお客様の場合は、移行前にそれらをアンインストールし、移行が正常に完了した後に再インストールすることを強くお勧めします。そうしないと、移行が失敗する可能性があります。

レプリケーションを設定しているお客様は、移行前に、[pg_upgradeのドキュメント](#)の手順に従う必要があります。そこで説明されている準備が行われていない場合、移行はおそらく成功しますが、レプリケーションの設定が壊れます。

重要: 移行を開始する前に:

- ・ システムカタログのデータコピーによるディスクの使用に起因する予期しない問題を回避するため、10%ほどの余裕をディスク容量に確保してください。
- ・ ディスク容量が不足するとLinuxシステムが中断する可能性があるため、ルートディレクトリの容量とボリウムマウントを確認してください。

synossysctlを使用して2022.2.0に更新すると、次のタスクが実行されます。

- ・ Black Duckインスタンスを停止する
- ・ Black Duck提供のPGコンテナのユーザー向けにデータベース移行ジョブを実行する
- ・ インスタンスを更新して再起動する

KubernetesおよびOpenShiftユーザーの場合:

- ・ 移行は1回限りのジョブによって実行されます。
 - ・ Black Duckを停止します。例:

```
kubect1 scale --replicas=0 -n <your_namespace> deployments --selector app=blackduck
```
 - ・ アップグレードジョブを実行します。例:

```
helm upgrade <your_deployment_name> .-n <your_namespace> <your_normal_helm_options> --set status=Stopped --set runPostgresMigration=true
```
 - ・ helm upgradeを使用して、Black Duckを通常どおり再起動します。
 - ・ この移行により、CentOS PostgreSQLコンテナの使用がBlack Duck提供のコンテナに置き換えられます。また、synopsys-initコンテナは、blackduck-postgres-waiterコンテナに置き換えられます。
- ・ プレーンなKubernetesでは、アップグレードジョブのコンテナはルートとして実行されます。ただし、唯一の要件は、ジョブがPostgreSQLデータボリウムの所有者と同じUIDで実行されることです。
- ・ OpenShiftでは、アップグレードジョブは、PostgreSQLデータボリウムの所有者と同じUIDで実行されることを前提としています。

Swarmユーザーの場合:

- ・ 移行は完全に自動化されているため、Black Duckの標準アップグレードの操作以外に追加の操作は必要ありません。
- ・ 上記のレイアウトとUIDの変更を行うには、blackduck-postgres-upgraderコンテナをルートとして実行する必要があります。
- ・ その後のBlack Duckの再起動時に、blackadu-postgres-upgraderは移行が不要であると判断し、すぐに終了します。
- ・ オプション: 移行が成功した後は、blackduck-postgres-upgraderコンテナをルートとして実行する必要はありません。

更新したセキュリティリスクランキング

一般的な業界動向に基づいて、デフォルトのセキュリティリスクランキングでは、脆弱性スコアの精度を高めるため、CVSS 3.0スコアをBDSAとともに主要スコアメトリックとして使用するようになりました。

新しいデフォルトのランキングは次のとおりです。

- ・ BDSA(CVSS v3.x)

- ・ NVD (CVSS v3.x)
- ・ BDSA (CVSS v2)
- ・ NVD (CVSS v2)

この更新では、新規インストールのランキングのみが変更されます。既存のインスタンスへのアップグレードでは、以前に設定されたランキング順序が維持されます。

バージョン詳細コンポーネントレポートの機能強化

新しい[コンポーネントリンク]列がバージョン詳細コンポーネントレポートに追加されました。この列には、コンポーネントの詳細ページを表示するときに表示されるコンポーネントのURLが含まれます。このレポートは、ダッシュボードで目的のプロジェクトを選択し、バージョンを選択し、[レポート]タブをクリックして、[作成]ボタンをクリックし、[バージョン詳細レポート]を選択することによって生成されます。次のポップアップで、[コンポーネント]チェックボックスがオンになっていることを確認し、新しい[コンポーネントリンク]列を含むコンポーネントレポートを生成します。

脆弱性警告表示の機能強化

プロジェクトのコンポーネントの脆弱性を表示するとき、当該の脆弱性のリンク済みBDSAが、このプロジェクトバージョンで使用されるコンポーネントのバージョンに関連付けられていない場合に、Black Duckが警告を表示するようになります。指定した脆弱性を表示すると、次のいずれかのメッセージが表示されます。

関連するNVDレコードがBDSAの脆弱性に存在しない場合：

Black Duck Security Advisory (BDSA) チームは、〈脆弱性ID〉をこのコンポーネントバージョンにマッピングしましたが、これはNational Vulnerability Database (NVD) の関連レコードには含まれていませんでした。

関連するBDSAレコードがNVDの脆弱性に存在しない場合：

National Vulnerability Database (NVD) は、〈脆弱性ID〉をこのコンポーネントバージョンにマッピングしましたが、Black Duck Security Advisory チームは、これは影響を受けていないと判断しました。

BDSAの脆弱性の詳細については、Black Duckのヘルプドキュメントを参照してください。

JobRunnerヒープおよびCPUベースのスロットル

Black Duck 2022.2.0以降、JobRunnerコンテナはヒープとCPUの使用状況を監視し、現在のリソース使用状況に基づいてワークロードを削減できるようになります。たとえば、ヒープ使用率が90%を超えた場合、JobRunnerはメモリリソースが回復するまでそれ自体を一時停止することができます。リソースが使用可能になると、JobRunnerは使用可能なリソースに比例してワークロードを増加します。

JobRunnerが一時停止した場合は、[管理] > [診断] > [システム情報] > [JobRunner] ページに表示されます。次のようなエントリが表示されます。

1 アクティブ JobRunner エンドポイント：

```
docker-swarm.jobrunner_1.docker-warm_default/58993e70a84c(172.23.0.15), paused=true
```

“paused=true”は、このJobRunnerがリソース制約の結果としてこれ以上作業していないことを示します。リソース使用率が回復すると、エントリはpaused=falseに変わり、JobRunnerは新しい作業を開始します。

ソースレポートでの無視されたスニペット

無視されたスニペットがソースレポートに含まれるように環境を設定できるようになりました。これは、環境変数INCLUDE_IGNORED_COMPONENTS_IN_REPORT=TRUEを設定することによって実行できます。

コンポーネント検索バージョン数の機能強化

プロジェクトに追加するコンポーネントを検索するときに、特定のコンポーネントにあるバージョンの数を確認できるようになります。この数は、コンポーネント名を入力すると動的に検索結果に表示されます。

セキュリティ脆弱性修正の機能強化

プロジェクトの修正ステータスを変更しようとする際の混乱を防ぐために、セキュリティの脆弱性を修正するプロセスが明確化されました。プロジェクトのセキュリティ脆弱性を表示するときに、ハッシュ化された行が表示され、修正対象として選択できない場合があります。これは、BDSAまたはCVEのいずれかのリンクタイプのセキュリティ脆弱性レコードがプロジェクトにあることが原因です。セキュリティリスクランキングでその脆弱性レコードの優先順位が高くない場合、そのプロジェクトに対して修正計画は実行できません。優先順位の高いセキュリティ脆弱性レコードに切り替えると、そのプロジェクトの修正計画を更新できるようになります。

プロジェクトバージョンのクローン作成の機能強化

プロジェクトバージョンのクローンを作成するときに、ディープライセンスデータを含めることができるようになりました。これを行うには、ダッシュボードでプロジェクトを選択し、プロジェクトのバージョンを表示しているときに[設定]タブをクリックします。

プロジェクトタグでの検索

[検索]ページでタグによってプロジェクトを検索および選択できるようになりました。これにより、タグでグループ化されたプロジェクトに対して保存済み検索の作成が可能になり、タグで識別される共通アプリケーション内にあるプロジェクトのダッシュボードがサポートされます。

ポリシーの新しい脆弱性条件ルール

脆弱性IDの新しいポリシー条件が追加されました。新しいポリシー条件では、特定の脆弱性(CVEまたはBDSA)IDをターゲットにしてコンポーネントにフラグを付けられるようにするポリシーを作成または編集できます。

新しいソフトウェア構成表(SBOM)レポートSPDX形式

プロジェクトのソフトウェア構成表レポートをSPDX形式でエクスポートできるようになりました。これを行うには、プロジェクトバージョンを表示して[レポート]タブをクリックし、[レポートの作成]ボタンをクリックします。現在は、SPDX 2.2をサポートしており、今後のBlack Duckバージョンでは、他の形式もサポートする予定です。

強化された署名スキャンリクエストボリューム管理

強化された署名スキャンで特定の期間に発生する可能性のある大量のリクエストをより適切に管理するため、スキャンサービスは最大動作限度に達した場合、クライアントで処理されるようにHTTP 429 (TOO MANY REQUESTS) エラーを返すようになりました。この場合、クライアントは10分間、30秒ごとに再試行してから、スキャンが失敗したことを通知します。

[検索]ページの新しいソートオプション

[検索]ページの[プロジェクトグループ]でプロジェクトをソートできるようになり、組織内の特定のプロジェクトグループに割り当てられているプロジェクトを簡単に検索できるようになりました。

/api/search/project-versions用の新しいprojectGroupMembershipフィルタ

このフィルタを使用すると、特定のプロジェクトグループの下位にあり、他のフィルタで指定された条件に一致するすべてのプロジェクトバージョンが返されます。projectGroupMembershipフィルタは、ユーザーがアクセス権を持つプロジェクトグループのみを返します。使用例は/api/search/projectversions?filter=projectGroupMembership:PG~{projectId}です。

レポートデータベースの機能強化

レポートスキーマに新しいビューが追加されました。

- ・ `reporting.scan_view`

Black DuckとIdentity Provider (IdP)間の保護された通信

Black Duckは、SAML認証要求に署名するための5年の有効期間を持つ自己署名証明書を作成するようになりました。管理者は、[管理者] > [システム設定] > [ユーザー認証]に移動し、[外部認証]セクションで[SAML]を選択し、[署名付き認証要求を送信]チェックボックスをオンにすることで、要求に署名する必要があるかどうかを設定できます。

このオプションのデフォルト設定はオフになっているか、不要です。有効にすると、Black Duck公開証明書をダウンロードするリンクが利用可能になり、IdPが認証要求を確認できるようにユーザーにこのリンクを配布する必要があります。

既知のコンポーネントへの一致しないコンポーネントの割り当て

構成表スキャン中に検出された一致しないコンポーネントを既知のコンポーネントに割り当てることができるようになりました。

新しい高速スキャンコンポーネントの依存関係ツリー

高速スキャン出力でプロジェクト内の脆弱なコンポーネントのインスタンスすべての依存関係ツリーを表示するようになりました。これにより、そのコンポーネントが、他の参照コンポーネントやサブプロジェクトなどでどのように参照されているかを明確に確認できます。3つの親依存関係を持つjackson-core コンポーネントの高速スキャンの例は次のようになります。

```
"componentName": "jackson-core",
"versionName": "2.9.6",
"dependencyTrees": [
[
"io.jitpack:module2:2.0-SNAPSHOT:module2:maven",
"com.fasterxml.jackson.module:jackson-module-kotlin:2.9.6",
"com.fasterxml.jackson.core:jackson-databind:2.9.6",
"com.fasterxml.jackson.core:jackson-core:2.9.6"
]
],
```

プロジェクトグループの役割名の更新

プロジェクトグループに関連付けられた役割の名前が更新され、「プロジェクトグループ」という表現が削除されました。役割の機能は、この更新では変更されていません。役割がどのように更新されたかについては、以下のリストを参照してください。

- ・ プロジェクトグループマネージャー→プロジェクトマネージャ
- ・ プロジェクトグループセキュリティマネージャー→セキュリティマネージャ
- ・ プロジェクトグループ構成表アノテーター→構成表アノテーター
- ・ プロジェクトグループ構成表マネージャー→構成表マネージャ
- ・ プロジェクトグループコードスキャナ→プロジェクトコードスキャナ

- ・ プロジェクトグループポリシー違反レビュー担当者→ポリシー違反レビュー担当者
- ・ プロジェクトグループビューア→プロジェクトビューア

プロジェクトおよびプロジェクトグループ管理の機能強化

複数のユーザーとプロジェクトグループをプロジェクトやプロジェクトグループに簡単に追加できるようになりました。ユーザーまたはプロジェクトグループの1回の追加操作で複数を選択できるように、ドロップダウンメニューが拡張されました。

Logstashコンテナメモリの増加

メモリ不足の問題によってクラッシュまたは再起動が発生する可能性があるため、Logstashコンテナに割り当てられるメモリを1024 MBから2560 MBに増やしました。これにより、操作に影響が及ぶWebアプリケーションの中断が減少します。

プロジェクトグループの削除の機能強化

既存のポリシールール式で参照されているプロジェクトグループは、削除できなくなりました。

文字列検索時の新しい拡張子の追加

ナレッジベースでのFLLD/FLCDスキャンとの拡張子の互換性を維持するために、以下の拡張子が、文字列検索で有効な拡張子のリストに追加されました。

- ・ pkginfo
- ・ properties
- ・ pc

サポートされるブラウザのバージョン

- ・ Safariバージョン15.0(16612.1.29.41.4、16612)
 - ・ Safariバージョン13.0以前はサポートされなくなりました
- ・ Chromeバージョン94.0.4606.71(公式ビルド)(x86_64)
 - ・ Chromeバージョン71以前はサポートされなくなりました
- ・ Firefoxバージョン92.0.1(64ビット)
 - ・ Firefoxバージョン71以前はサポートされなくなりました
- ・ Microsoft Edgeバージョン94.0.992.38(公式ビルド)(64ビット)
 - ・ Microsoft Edgeバージョン78以前はサポートされなくなりました

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:11-2.7
- ・ blackducksoftware/blackduck-authentication:2022.2.0
- ・ blackducksoftware/blackduck-webapp:2022.2.0
- ・ blackducksoftware/blackduck-scan:2022.2.0
- ・ blackducksoftware/blackduck-jobrunner:2022.2.0
- ・ blackducksoftware/blackduck-cfssl:1.0.5
- ・ blackducksoftware/blackduck-logstash:1.0.16

- `blackducksoftware/blackduck-registration:2022.2.0`
- `blackducksoftware/blackduck-nginx:2.0.12`
- `blackducksoftware/blackduck-documentation:2022.2.0`
- `blackducksoftware/blackduck-upload-cache:1.0.21`
- `blackducksoftware/blackduck-redis:2022.2.0`
- `blackducksoftware/blackduck-bomengine:2022.2.0`
- `blackducksoftware/blackduck-matchengine:2022.2.0`
- `blackducksoftware/blackduck-webui:2022.2.0`
- `sigsynopsys/bdba-worker:2021.12.1`
- `blackducksoftware/rabbitmq:1.2.6`

APIの機能強化

新規または変更されたAPIリクエストの詳細については、Black Duckで入手可能なAPIドキュメントを参照してください。

新しい署名付き認証要求フィールド

Black Duckが署名付き認証要求をIdPに送信するかどうかを判断するために、新しい`sendSignedAuthenticationRequest`フィールドが以下のAPIリクエストに追加されました。このフィールドのデフォルト値はFALSEです。証明書をダウンロードするためのメタリンクは、署名付き認証要求構成がTRUEに設定されている場合にのみ使用できます。

- `GET, POST /api/sso/configuration`

新しい`/api/active-users`エンドポイント

この新しいクエリは、指定された日付以降にシステムにログインしたユーザーのすべてのユーザー最終ログイン情報を返します。このクエリでは、休眠ユーザーと同じ`sinceDays`クエリパラメータを使用します。

新規プロジェクトバージョンレポートのエンドポイント

タイプ(通知ファイル、バージョンレポート、脆弱性修正、脆弱性ステータス、脆弱性更新、ソフトウェア構成表レポート)に関係なくすべてのバージョンレポートをサポートするために、次のパブリックエンドポイントが追加されました。

- `GET /api/projects/{projectId}/versions/{projectVersionId}/reports`
- `GET /api/projects/{projectId}/versions/{projectVersionId}/reports/{reportId}`
- `DELETE /api/projects/{projectId}/versions/{projectVersionId}/reports/{reportId}`
- `GET /api/projects/{projectId}/versions/{projectVersionId}/reports/{reportId}/contents`
- `GET /api/projects/{projectId}/versions/{projectVersionId}/reports/{reportId}/download`

新しいポリシールールパブリックエンドポイント

アクティブなポリシールールを取得するために、新しいパブリックAPIリクエストが追加されました。

- `GET /api/projects/{projectId}/versions/{projectVersionId}/policy-rules`

新しい/api/cpes/{cpeId}/originsエンドポイント

Black Duck 2022.2.0では、/api/cpes/{cpeId}/variantsエンドポイントが廃止され、/api/cpes/{cpeId}/originsに置き換えられます。/api/cpes/{cpeId}/variantsは、Black Duck 2022.4.0で削除されます。/api/cpesのメタデータ内のAPIリンクも、/api/cpes/{cpeId}/variantsではなく、/api/cpes/{cpeId}/originsを返すように更新されています。

APIリクエストのページ制限の最大値

システムリソースの使用量を抑えるために、次のAPIリクエストにページ制限の最大値が設定されるようになりました。この制限は現在1000項目に設定されています。

- GET /api/projects/<id>/versions/<id>/components
- GET /api/projects/<id>/versions/<id>/vulnerable-bom-components
- GET /api/codelocations
- GET /api/projects/<id>/versions
- GET /api/projects
- GET /api/users

APIエンドポイント用の新しいソートフィルタ

parentProjectGroupNameという新しいソートオプションが次のAPIエンドポイントに利用できるようになりました。これにより、親プロジェクトグループ名でプロジェクトバージョンをソートできます。

- /api/search/project-versions
- /api/watched-projects
- /api/dashboards/users/{id}/saved-searches/{id}

新しいGET /api/scan-readiness APIエンドポイント

すべてのスキャンコンテナの準備状態を取得する新しいパブリックAPIエンドポイントが追加されました。

- GET /api/scan-readiness

応答例:

```
{
  "readiness": "ACCEPTING",
  "items": [
    {
      "id": "9dc7653a462b",
      "service": "scan",
      "readiness": "ACCEPTING",
      "updatedAt": "2021-12-21T17:26:01.495Z",
      "versionId": 1
    }
  ]
}
```

- マルチスキャンレプリカ環境で、すべてのスキャンコンテナレプリカが正常な場合、集約状態はACCEPTINGになります。システムは、新しいスキャンを問題なく受け入れて処理できます。
- マルチスキャンレプリカ環境で、1つのスキャンコンテナが正常ではなく、他のレプリカが正常な場合、集約状態はPARTIALになります。この状態では、システムが過負荷になります。スキャンパフォーマンスが低下する可能性があります。スキャンは、タイムアウトまたは失敗する可能性があります。

- ・ マルチスキャンレプリカ環境で、一部のスキャンコンテナが正常ではない場合、集約状態はDEGRADEDになります。システムは過負荷状態になり、新しいスキャンを受け入れられません。拒否するように設定すると、新しいスキャン要求は受け入れられなくなり、HTTP 429リターンコードが返されます。
- ・ コンテナがダウンした場合、そのエントリは5分後(間隔は設定可能)に削除されます。

GET /api/codelocations/{codeLocationId}/scan-summariesの応答の更新

/api/codelocations/{codeLocationId}/scan-summariesに対して生成されたAPI応答内のscanType値は、あいまいさを避けるために各タイプに分割されるようになりました。新しい値には、次のものが含まれます。

- ・ PACKAGE_MANAGER
- ・ BINARY
- ・ BOM_IMPORT
- ・ SIGNATURE

従来のスキャンでは、scanType値にBDIOが引き続き使用されます。

この変更はBlack Duck 2021.8.0で導入されているので注意してください。

2022.2.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (HUB-31267)。グローバルな役割を持たないユーザーが、スキャンページまたはプロジェクトURLから直接すべてのプロジェクトにアクセスできていた問題が修正されました。スキャン権限のないユーザーには、projects/.../versions/.../codelocations画面に[スキャンのアップロード]ボタンが表示されなくなりました。
- ・ (HUB-31734)。[コンポーネント]ページのフィルタがプロジェクト レベルのユーザーには機能していなかった問題を修正しました。
- ・ (HUB-31993)。アップロードされたBDIOファイルのバージョン/リリース値がnullの場合にスキャンが失敗する可能性があった問題を修正しました。バージョン/リリース値がない場合でも、スキャンは失敗しなくなりました。
- ・ (HUB-31964)。JDBCクエリのパラメータが多すぎた結果としてプロジェクトバージョンのVersionReportJobが失敗することにより、一部のレポートが生成できなかった問題が修正されました。
- ・ (HUB-30479、HUB-31842)。優先順位の低い脆弱性レコードを修正に使用したときに、BDSAとCVEレコードの両方を含む脆弱性の修正が機能していなかった問題が修正されました。脆弱性を修正するには、優先順位の高い脆弱性レコードタイプを使用する必要があります。
- ・ (HUB-31207)。アーカイブされたプロジェクト下の脆弱性を修正しても、一度適用されたセキュリティ上のリスクの数は更新されなかった問題が修正されました。アーカイブされたプロジェクトバージョンの脆弱性をユーザーが修正することはできないため、プロジェクトバージョンがアーカイブされたら、脆弱性修正の[更新]ボタンはグレー表示にされるようになりました。
- ・ (HUB-32029)。一部の「無視された」コンポーネントが、再スキャン後に「無視を解除」になる可能性があった問題が修正されました。
- ・ (HUB-31768)。通知ファイルの生成時に、無視されたスニペットに基づいた著作権が誤って含まれていた問題が修正されました。
- ・ (HUB-32296、HUB-32255)。REST API GET /api/vulnerabilities/CVE-2021-44228/affected-projectsが0項目を返すという問題が修正されました。また、検索結果とエンドポイントの両方の、影響を受けるプロジェクト数では、関連する脆弱性を持つコンポーネントもカウントされるようになったことにも注意してください。
- ・ (HUB-31801、HUB-32424)。著作権の[更新]ボタンがスーパー ユーザーのロールに表示されていた問題を修正しました。この機能は、著作権を更新する権限を持つ役割にのみ表示されるようになりました。

- ・ (HUB-32692)。コンポーネントに複数の脆弱性があり、それぞれの脆弱性ステータスが異なる場合、コンポーネントのすべての脆弱性が選択したポリシー ルールに一致しない限り、ポリシー ルールがポリシー違反をトリガーしない可能性があった問題を修正しました。
- ・ (HUB-32357)。コンポーネントのKB更新、コンポーネントのバージョン、ライセンス、NVD脆弱性、およびBDSA脆弱性を処理するナレッジベースアクティビティジョブに関する問題が修正されました。これまでは、エラーや問題が発生した場合、該当するすべてのプロジェクトバージョンで単一の更新を処理することにフォールバックしていました。この場合、多くのチャーンが発生し、KB更新ジョブの処理速度が低下する可能性があります。
- ・ (HUB-32543)。プロジェクトマネージャとプロジェクトグループマネージャの役割を割り当てることにより、プロジェクトマネージャの役割に対する設定がオフになった場合に、これらの役割がポリシーを上書きし、脆弱性を修正する可能性があった問題が修正されました。セキュリティ上の役割は、これらの権限を持つプロジェクトマネージャまたはスーパーユーザーによってのみ割り当てることができるようになりました。
- ・ (HUB-31129)。Hubでのプロジェクトバージョンレポート(脆弱性の詳細レポートなど)に印刷される脆弱性のURLに、BDSAレコードを含むCVEが含まれる(コンポーネントにもBDSAレコードがある場合)可能性があった問題が修正されました。BDSA番号が付加されたCVEリンクは、脆弱性レポートに印刷されなくなります。
- ・ (HUB-31044)。カスタムフィールドID値が正しくないAPIを使用してポリシーを設定すると、後でポリシー画面が正しく表示されなくなる可能性があった問題が修正されました。
- ・ (HUB-31753)。CollectScanStatsJobジョブが完了するまでに予想よりも時間がかかり、データベースの不要な肥大化を招く可能性があった問題が修正されました。
- ・ (HUB-31663)。QuartzSearchDashboardRefreshJobが、このジョブの複数インスタンスをスケジュールしようとして、データベースへのクエリが大量にブロックされる可能性があった問題が修正されました。
- ・ (HUB-31862)。日本語ローカライゼーションで構成表アノテーターの役割に関する翻訳が欠落していた点が修正されました。
- ・ (HUB-31208)。構成表およびコンポーネントバージョンセキュリティタブではIBM COS SDK For Java 2.10.0コンポーネントが脆弱であると表示されていたのに、コンポーネントバージョンページでは脆弱性が表示されていなかった問題が修正されました。
- ・ (HUB-31735)。レポート(source.csv)と[ソース]ページ間のスニペット レコードの不一致に関する問題を修正しました。無視されたスニペットがレポートに含まれている場合は、INCLUDE_IGNORED_COMPONENTS_IN_REPORT環境変数も機能するようになりました。
- ・ (HUB-31566)。ジョブのオーバースケジュール、メモリ不足問題、および/または長時間のジョブにより、サービスでデータベース接続エラーが発生する可能性があった問題が修正されました。
- ・ (HUB-31997)。json-schema v0.3.0コンポーネントの脆弱性情報が修正されました。
- ・ (HUB-32527)。通知ファイルレポートを作成するときに、次のモдалで正しくないレポートタイプ名が表示される可能性があった問題が修正されました。
- ・ (HUB-31750)。BDSA-2021-0395ページに表示されていた壊れたリンクが修正されました。
- ・ (HUB-31976)。「スーパーユーザー」の役割を持つユーザーが、プロジェクトバージョンスキャンページ内でスキャンを管理できなかった問題が修正されました。
- ・ (HUB-32566)。ユーザーがファイルをApache Pulsarコンポーネントにマッピングできなかった問題が修正されました。
- ・ (HUB-31201)。プロジェクト(グループ)ビューアの役割のみでユーザーをプロジェクト(グループ)に割り当てることができなかった問題が修正されました。
- ・ (HUB-31251)。カスタムフィールドオプションを削除するとポリシーAPIが壊れる可能性があった問題が修正されました。
- ・ (HUB-29676、HUB-32912)。[コンポーネントの追加/編集]ダイアログ ボックスで、一部のコンポーネントのバージョンを選択できなかった問題を修正しました。

- ・ (HUB-30847)。webappコンテナが非ルートユーザーとして実行されたときに、webapp-logstashポッドで権限拒否エラーが発生しクラッシュしていた問題が修正されました。
- ・ (HUB-31375)。プロジェクト概要の「最終更新日」と、[検索] > [プロジェクト]の「更新日」の値が一致していなかった問題を修正しました。
- ・ (HUB-30004)。Detectを使用した正常なバイナリスキャンによってHUB上で空の構成表が生成される可能性があった、OpenShift環境での権限の問題が修正されました。
- ・ (HUB-32159)。カスタム署名レベルに空の値を送信すると、誤ったエラーメッセージが生成される可能性があった問題が修正されました。
- ・ (HUB-32142)。権限がないためにRabbitMQがOpenShiftにインストールできない可能性があった問題が修正されました。
- ・ (HUB-32216)。ユーザーがコンポーネントのポリシー違反を上書きしようとし、その後特定のバージョンでそのコンポーネントバージョンのポリシー違反を元に戻そうとしても何も起こらない可能性があった問題が修正されました。
- ・ (HUB-32312)。KBUpdateWorkflowジョブコンポーネントバージョン更新でメモリを飽和させ使い切ってしまう、タイムスタンプを進められない可能性があった問題が修正されました。
- ・ (HUB-31916)。UIページが更新されるまで、プロジェクト設定更新APIが有効ではないように見える可能性があった問題が修正されました。
- ・ (HUB-30088)。SSOアカウントからログアウトするときにログアウトページが表示されなかった問題が修正されました。
- ・ (HUB-32442)。依存関係パスの取得に使用されたAPIクエリの完了が、予想よりも大幅に時間がかかっていた問題が修正されました。
- ・ (HUB-32538、HUB-32541)。kbUpdateJobが失敗し、詳細な更新にフォールバックして、完了までに大幅に時間がかかる可能性があった問題が修正されました。
- ・ (HUB-32708)。実行に時間がかかり、PostgreSQL 11を実行しているAzureシステムで全体的な速度低下を引き起こしていた、Black Duck 2021.10.0で導入された統計クエリが削除されました。この問題は、問題を調査しているMicrosoftのサポート担当者から報告されています。その他のインストールは、この問題の影響を受けません。
- ・ (HUB-32364、HUB-31606)。テーブルに15を超えるスキャンがあり、ユーザーがそれらを一括削除しようとした場合に、スキャンページがフリーズして応答なくなる可能性があった問題が修正されました。
- ・ (HUB-32602)。IPコードパスを介して行われたパッケージマネージャスキャンの現在のスキャンステータスが、ScanPurgeJobプロセスにより誤ってFAILEDに変更される可能性があった問題が修正されました。
- ・ (HUB-31122)。ScanPurgeJobプロセスがバックグラウンドで実行されているために、BomEngineでスキャンがスキップされることがあった問題が修正されました。
- ・ (HUB-30882)。レポートの脆弱性修正のターゲットの日付/実際の日付が、タイムゾーン変換のために入力した日付より1日前になる可能性があった問題を修正しました。
- ・ (HUB-32434)。ベルアイコンをクリックしてすべての通知を表示してから、通知を生成したプロジェクト名をクリックするとエラーが発生していた問題が修正されました。
- ・ (HUB-32027)。日本語のローカライゼーションで推移的な依存関係バイナリに対する間違った翻訳が修正されました。
- ・ (HUB-30788)。タイプに関係なくすべてのバージョンレポートをサポートする新しいエンドポイントが追加されました。詳細については、上記の「APIの機能強化」のセクションを参照してください。
- ・ (HUB-32843)。日本語のローカライゼーションで、プロジェクト バージョン ページの[コンポーネント]タブにおける「スニペット」の翻訳の欠落を修正しました。

- ・ (HUB-31964)。JDBCのパラメータが多すぎた結果としてプロジェクトバージョンのVersionReportJobが失敗することにより、一部のレポートが生成できない可能性があった問題が修正されました。
- ・ (HUB-32393)。構成表にスニペット マッチが存在する場合、結果がフィルタされても上位ビューにセキュリティ/ライセンス/運用上のリスクが設定されないことがあった問題を修正しました。
- ・ (HUB-32604)。環境変数BLACKDUCK_CORS_ALLOWED_ORIGINS_PROP_NAMEがワイルドカードに設定されている場合、CORS機能が動作しない可能性があった問題が修正されました。

Black Duck 2021.10.x

バージョン2021.10.3の発表

Apache Log4j2のセキュリティアドバイザリ(CVE-2021-45046およびCVE-2021-45105)

Apache Organizationは、Log4j2コンポーネントの新しいバージョン(2.17.0)をリリースしました。これは、バージョン2.15.0および2.16.0で修正されていない追加の脆弱性に対処するものです。

[CVE-2021-45046](#)では、コンテキストルックアップまたはスレッドコンテキストマップパターンのいずれかを使用するデフォルト以外のパターンレイアウトが、ログ構成で使用されているときに、攻撃者がスレッドコンテキストマップ(MDC)入力データを制御して、JNDIルックアップパターンを使った悪意のある入力データを作成することができ、その結果サービス拒否(DOS)攻撃が引き起こされます。

[CVE-2021-45105](#)では、攻撃者がスレッドコンテキストマップ(MDC)入力データを制御して、再帰的なルックアップを含む悪意のある入力データを作成でき、その結果、プロセスを終了させるStackOverflowErrorが発生し、サービス拒否(DOS)攻撃が引き起こされます。

詳細については、[ApacheのLog4jセキュリティ脆弱性のページ](#)を参照してください。

Black Duck 2021.10.2バージョンで述べられているように、Black Duckの製品、サービス、システムに対する露出は限定的であると考えられます。露出があった範囲に対しては、状況を修正済みであるか、または修正の過程にあります。今後の更新については、[コミュニティページ](#)を引き続きご確認ください。

バージョン2021.10.3の新機能および変更された機能

Log4jの更新

Apache Log4j 2 Javaライブラリは、重要なCVE-2021-45046およびCVE-2021-45105の脆弱性に対処するために2.17.0に更新されました。

Logstashの更新

Black Duckで使用されるLogstashイメージは、Log4j2バージョン2.17.0を使用する7.16.2にアップグレードされました。

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:9.6-1.4
- ・ blackducksoftware/blackduck-authentication:2021.10.3
- ・ blackducksoftware/blackduck-webapp:2021.10.3
- ・ blackducksoftware/blackduck-scan:2021.10.3
- ・ blackducksoftware/blackduck-jobrunner:2021.10.3
- ・ blackducksoftware/blackduck-cfssl:1.0.4

- blackducksoftware/blackduck-logstash:1.0.15
- blackducksoftware/blackduck-registration:2021.10.3
- blackducksoftware/blackduck-nginx:2.0.9
- blackducksoftware/blackduck-documentation:2021.10.3
- blackducksoftware/blackduck-upload-cache:1.0.19
- blackducksoftware/blackduck-redis:2021.10.3
- blackducksoftware/blackduck-bomengine:2021.10.3
- blackducksoftware/blackduck-matchengine:2021.10.3
- blackducksoftware/blackduck-webui:2021.10.3
- sigsynopsys/bdba-worker:2021.9.2
- blackducksoftware/rabbitmq:1.2.5

2021.10.3で修正された問題

このリリースでは、次の問題が修正されています。

- (HUB-32233)。CVE-2021-45046およびCVE-2021-45105に対応して、Log4jをバージョン2.17.0にアップグレードしました。
- (HUB-32295)。Bitnami LogstashをLog4j 2.17.0を使用する7.16.2バージョンに更新しました。

バージョン2021.10.2の発表

Apache Log4J2のセキュリティアドバイザリ(CVE-2021-44228)

Black Duck は、プロジェクトのGitHubを介して2021年12月9日に公開された、Log4Shell(またはLogJam)と呼ばれるオープンソースのApache Log4j 2 Javaライブラリに関連するセキュリティの問題を認識しています。この脆弱性により、認証されていないリモートコードの実行が可能になり、Apache Log4j 2バージョン2.0~2.14.1に影響が及んでいます。詳細については、[CVEの公式投稿](#)を参照してください。

現時点でわかっている知見に基づいて、Black Duckの製品、サービス、システムに対する露出は限定的であると考えています。露出があった範囲に対しては、状況を修正済みであるか、または修正の過程にあります。今後の更新については、[コミュニティページ](#)を引き続きご確認ください。

<https://www.synopsys.com/blogs/software-security/zero-day-exploit-log4j-analysis/>も参照してください。

バージョン2021.10.2の新機能および変更された機能

Log4jの更新

Apache Log4j 2 Javaライブラリは、重要なCVE-2021-44228の脆弱性に対処するために2.15.0に更新されました。

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.4
- blackducksoftware/blackduck-authentication:2021.10.2
- blackducksoftware/blackduck-webapp:2021.10.2
- blackducksoftware/blackduck-scan:2021.10.2
- blackducksoftware/blackduck-jobrunner:2021.10.2

- ・ blackducksoftware/blackduck-cfssl:1.0.4
- ・ blackducksoftware/blackduck-logstash:1.0.13
- ・ blackducksoftware/blackduck-registration:2021.10.2
- ・ blackducksoftware/blackduck-nginx:2.0.9
- ・ blackducksoftware/blackduck-documentation:2021.10.2
- ・ blackducksoftware/blackduck-upload-cache:1.0.19
- ・ blackducksoftware/blackduck-redis:2021.10.2
- ・ blackducksoftware/blackduck-bomengine:2021.10.2
- ・ blackducksoftware/blackduck-matchengine:2021.10.2
- ・ blackducksoftware/blackduck-webui:2021.10.2
- ・ sigsynopsys/bdba-worker:2021.9.2
- ・ blackducksoftware/rabbitmq:1.2.5

2021.10.2で修正された問題

このリリースでは、次の問題が修正されました。

- ・ (HUB-32174)。CVE-2021-44228に対応して、Log4jをバージョン2.15.0にアップグレードしました。

バージョン2021.10.1の新機能および変更された機能

RestResponseErrorHandlerの改善

RestResponseErrorHandlerは、Black Duck機能の信頼性を向上させるために、ナレッジベースおよびネットワーク内の他のサーバーからの予期しない応答をより適切に処理できるようになりました。

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:9.6-1.4
- ・ blackducksoftware/blackduck-authentication:2021.10.1
- ・ blackducksoftware/blackduck-webapp:2021.10.1
- ・ blackducksoftware/blackduck-scan:2021.10.1
- ・ blackducksoftware/blackduck-jobrunner:2021.10.1
- ・ blackducksoftware/blackduck-cfssl:1.0.4
- ・ blackducksoftware/blackduck-logstash:1.0.11
- ・ blackducksoftware/blackduck-registration:2021.10.1
- ・ blackducksoftware/blackduck-nginx:2.0.9
- ・ blackducksoftware/blackduck-documentation:2021.10.1
- ・ blackducksoftware/blackduck-upload-cache:1.0.19
- ・ blackducksoftware/blackduck-redis:2021.10.1
- ・ blackducksoftware/blackduck-bomengine:2021.10.1
- ・ blackducksoftware/blackduck-matchengine:2021.10.1

- [blackducksoftware/blackduck-webui:2021.10.1](#)
- [sigsynopsys/bdba-worker:2021.9.1](#)
- [blackducksoftware/rabbitmq:1.2.5](#)

2021.10.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-31129)。Hubでのプロジェクトバージョンレポート(脆弱性の詳細レポートなど)に印刷される脆弱性のURLに、BDSAレコードを含むCVEが含まれる(コンポーネントにもBDSAレコードがある場合)可能性があった問題が修正されました。BDSA番号が付加されたCVEリンクは、脆弱性レポートに印刷されなくなります。
- (HUB-31293)。2021.8.xにアップグレードした後、Pythonの推移的な依存関係が直接的な依存関係に変更されていた問題が修正されました。
- (HUB-31764)。脆弱性の修正ステータスが更新されたときに、構成表の計算中にNullポインタ例外を引き起こしていた問題が修正されました。
- (HUB-30004)。Detectを使用した正常なバイナリスキャンによってHUB上で空の構成表が生成される可能性があった、OpenShift環境での権限の問題が修正されました。
- (HUB-31879)。構成表の作成フェーズ中にスキャンがスタックする可能性があった問題が修正されました。詳細については、上記の「新機能および変更された機能」セクションの「RestResponseErrorHandlerの改善」を参照してください。
- (HUB-31896)。パブリックAPIを介した構成表の脆弱性に対する修正の更新が、再スキャン後に持続していなかった問題が修正されました。
- (HUB-31753)。CollectScanStatsJobジョブが完了するまでに予想よりも時間がかかり、データベースの不要な肥大化を招く可能性があった問題が修正されました。
- (HUB-31663)。QuartzSearchDashboardRefreshJobが、このジョブの複数インスタンスをスケジュールしようとして、データベースへのクエリが大量にブロックされる可能性があった問題が修正されました。
- (HUB-31755)。プロジェクトバージョンレポートの生成時に、プロジェクト構造が循環しているためにVersionReportJobでメモリ不足になる可能性があった問題が修正されました。
- (HUB-31566)。ジョブのオーバースケジュール、メモリ不足問題、および/または長時間のジョブにより、サービスでデータベース接続エラーが発生する可能性があった問題が修正されました。

バージョン2021.10.0の発表

強化された署名スキャン

2021.8.0リリースのPackage Manager Scanningで導入されたパフォーマンス強化機能は、2021.10.0リリースの署名スキャンで利用可能になっています。これらの強化の主要部分は、重複する構成表の検出です。この機能を使用した場合、特定のプロジェクトおよびバージョンに関連付けられている構成表が署名スキャンによって変更されない限り、構成表の計算はバイパスされます。

さらに、強化された署名スキャンでは、新たなパッケージマネージャスキャンまたは署名スキャンの処理で、JobRunnerは役割を果たさなくなりました。強化された署名スキャンの実行では、システムリソースがさらに必要になることはありませんが、コンテナの微妙なバランス調整が必要になる可能性があります。バランス調整が必要かどうかについては、Black Duckのサポートにお問い合わせください。当社は強化された機能の活用をすべてのお客様に推奨しています。

Black Duck 2021.8.0ではDetect 7.4を明確化

完全な機能性と互換性を維持するには、Black Duckバージョン2021.8.0ではDetect 7.4が必要になります。Black Duckで旧バージョンのDetectは引き続き使用できますが、集約BDIOファイルの使用時に、依存関係タイプやソースビューの不整合が構成表内で生じる可能性があります。

Detect 7.4へのアップグレードで、構成表内の不整合を回避できます。

PostgreSQLコンテナの9.6から11への移行

Black Duck は、2022.2.0リリースでPostgreSQLイメージをバージョン9.6からバージョン11に移行します。Black DuckのPostgreSQLイメージを使用していないお客様には影響はありません。

Black Duck PostgreSQL 9.6の廃止

Black Duckは、Black Duck 2020.6.0リリースで表明したとおり、2021.6.0リリースで実装された外部PostgreSQL 9.6のサポートを終了することになりました。2022.2.0リリース以降の場合、Black DuckはPostgreSQL 9.6と連動しなくなります。さらにPostgreSQL 9.6インスタンスを参照している場合は、Black Duckが起動しなくなります。

PostgreSQLサポートのスケジュール

今後の2022.10.0リリース以降、Black Duckは外部PostgreSQL 11のサポートを終了します。今後のPostgreSQLバージョンに関しては、サポートの開始日と終了日を以下の表で確認してください。

PGバージョン	最初のリリース	最終リリース	BD外部サポートの追加	BD外部サポートの終了
16.x	2023年後半	2028年後半	2024.10.0	2026.10.0
15.x	2022年後半	2027年後半	2023.10.0	2025.10.0
14.x	2021年9月	2026年11月	2022.10.0	2024.10.0
13.x	2020年9月	2025年11月	2021.8.0	2023.10.0
12.x	2019年10月	2024年11月	X	X
11.x	2018年10月	2023年11月	2020.6.0	2022.10.0

2021.10.0以降にデータベースbds_hub_reportは廃止

2021.10.0以降、Black Duckの新インストールでは、bds_hub_reportデータベースが作成されなくなります。最終的に2022.10.0でbds_hub_reportを削除する予定です。

またbds_hub_reportが存在しない場合でも、hub_create_data_dump.shおよびhub_db_migrate.shスクリプト（当社のオーケストレーションファイルとともに配布）は正常に動作するようになります。

- ・ bds_hub_reportが存在する場合、それをhub_create_data_dump.shスクリプトはダンプしますが、存在しない場合でも、スクリプトがエラーになることはありません。bds_hub_reportが存在しない場合、スクリプトはスキップを通知するメッセージを出力します。
- ・ hub_db_migrate.shスクリプトは、bds_hub_reportが存在する場合（ダンプファイルが存在するかどうかに関係なく）、そのリストアを試行します（先行リリースの動作とマッチ）。bds_hub_reportが存在しない場合、ダンプファイルが存在するかどうかに関係なく、リストアは試行されません。

- ・ 新しいスクリプトhub_recreate_reportdb.shが追加されました。2021.8.x以前のbds_hub_report DBから2021.10.0以降の新インストールにデータをコピーする場合、この新しいスクリプトによってbds_hub_reportが再作成されます。この場合、次のようになります。
- ・ 以前のBDインスタンスでhub_create_data_dump.shを実行します。
- ・ 新しいBDインスタンスでhub_recreate_reportdb.shを実行します。
- ・ 新しいBDインスタンスでhub_db_migrate.shを実行し、ダンプはステップ#1で作成します。

APIリクエストに最大ページ数の制限を適用する予定

Black Duck 2022.2.0以降、APIリクエストには最大ページ数の制限が適用されます。単一のリクエストを作成する場合には、文書化されたページ制限以下の値で制限リクエストパラメータを指定する必要があります。文書化された制限を超えたページリクエストは切り捨てられ、許容される最大ページ数のみが返されます。ページサイズのリクエストは拒否されませんが、ページリクエストあたりの最大結果数が返されます。

アプリケーションの安定性を高め、不当に大きなリクエストによるパフォーマンスの低下を防ぐために、以降のリリースではこの制限が継続的に適用されます。

廃止されたAPI

以下の廃止されたエンドポイントは「404 NOT FOUND」エラーを返し、ターゲットリソースへのアクセスが利用できなくなったことを示します。

- ・ GET /oauthclients
- ・ POST /oauthclients
- ・ DELETE /oauthclients/{oauthClientId}
- ・ GET /oauthclients/{oauthClientId}
- ・ PUT /oauthclients/{oauthClientId}
- ・ POST /vulnerabilities/vulndb-copy

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.8.0が日本語にローカライズされました。

簡体字中国語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.8.0が簡体字中国語にローカライズされました。

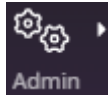
バージョン2021.10.0の新機能および変更された機能

強化された署名生成のエラーメッセージを更新

署名スキンのサーバー側エラーメッセージが更新されました。エラーメッセージの完全なリストは、今後のリリースのユーザーガイドに記載されます。

マップされていないスキャンデータの保持構成設定

マップされていないスキャンのデフォルト保持期間を管理者が変更できるように、新しい構成設定が利用可能になりました。Black Duck 2021.10.0以降、この設定はデフォルトで有効になり、期間は30日（以前は365日）に設定されます。この保持設定は更新でき、最も短い場合は1日、最も長い場合は365日に設定できます。




UIでこの設定を変更するには、**Admin** をクリックし、[設定]、[データの保管]の順にクリックします。

推定セキュリティリスク

この推定リスク統計は、セキュリティ脆弱性の重大度カテゴリ別にソートされたコンポーネントの全バージョンを参照し、コンポーネントバージョンごとに各重大度カテゴリの最大脆弱性数を計算することで算出されます。各重大度カテゴリの最大脆弱性数は、セキュリティリスクの構成表の[重大度カテゴリ別の推定セキュリティリスク]に表示されます。重大度が最高値になっているカテゴリ数は、複数の異なるコンポーネントバージョンを参照している可能性があります。以下に例を示します。

- バージョン1.1では、重大2、高3、中15、低4になっています
- バージョン1.2では、重大2、高4、中12、低1になっています
- この例で、コンポーネントのバージョンが不明の場合、重大度カテゴリ別の推定セキュリティリスクは、構成表上で重大2、高4、中15、低4になります。

推定リスクではなく、正確なリスクを表示するには、アプリケーションで使用されている正確なバージョンを選択する必要があります。この推定リスク情報は、どのコンポーネントを最初にレビューすべきかの優先順位付けに役立ちます。企業のセキュリティポリシーに基づいて優先順位をさらに明確にし、コンポーネントの最初の選別が実行できるように、推定リスク情報とともにBDポリシー管理を使用することをお勧めします。

 **注：** 表示される情報は統計データの推定のみです。結果的に、推定セキュリティリスクにはCVEデータは含まれません。



ディープライセンスデータが有効の場合に通知レポートを生成する



通知ファイルは、宣言されたライセンスを追加ライセンスの前に配置するようになりました。宣言されたライセンスと追加ライセンスは、アルファベット順にソートされます。

[ソース]ビューと[ソース]レポートにコメントを追加する

プロジェクトの[ソース]ビューでは、エントリにコメントを追加できるようになりました。ファイルコメントは、スニペットビューにも表示されます。ソースレポートでは、これらのコメントは「コメント」というラベルの付いた新しい列にも表示されます。ソースレポートを作成するには、[レポート]タブで[バージョン詳細レポート]の[ソース]チェックボックスをオンにします。


[ソース]タブの特定エントリに関するコメントは、次の方法で入力できます。

- そのコンポーネントの行の末尾にある  アイコンをクリックし、ドロップダウンメニューから[コメント]を選択します。また、すでにコメントがある場合は  アイコンをクリックします。


[ソース]ビューでエントリをクリックし、コンポーネントの名前をクリックします。次に  アイコンをクリックし、ドロップダウンメニューから[コメント]を選択します。また、すでにコメントがある場合は  アイコンをクリックします。

ポリシー管理の機能強化 – プロジェクトグループ

Black Duck ユーザーは、プロジェクトグループとその下位アイテムにポリシールールを適用できるようになりました。

適用するには、[ポリシー管理]に移動し、[ポリシールールの作成]ボタンまたは  ボタンをクリックして[編集]を選択します。[ポリシールールの作成/編集]モーダルが開いたら、[プロジェクトのサブセット。フィルタの内容...]オプションが有効になっており、[プロジェクトの条件]フィルタドロップダウンが表示されることを確認します。

ポリシー管理の機能強化 – 脆弱性条件に(RCE)リモートコード実行を追加

Black Duck ユーザーは、ポリシーの作成または編集時に、フィルタオプションとしてリモートコード実行(RCE)を追加できるようになりました。適用するには、[ポリシー管理]に移動し、[ポリシーールの作成]ボタンまたは  ボタンをクリックして[編集]を選択します。[脆弱性の条件]ドロップダウンメニューには、新しい(RCE)リモートコード実行の値が表示されます。

プロジェクトグループマネージャの権限の変更

以前は、脆弱性の修正やポリシーの上書きをプロジェクトマネージャに許可するグローバル設定によって、プロジェクトグループマネージャの実際の権限が影響を受けることはありませんでした。現在では、プロジェクトグループマネージャの役割の権限は、プロジェクトマネージャの役割設定に基づいて調整されるようになりました。

署名スキャナのドライラン更新

以前は、署名スキャナのドライランを実行すると、出力でJSONファイルが生成されていました。Black Duck 2021.10.0以降、生成される出力ファイルには.bdio拡張子が付けられ、zip形式で圧縮されています。出力ファイルは、従来の署名スキャンと同様に、今後もドライランと同じディレクトリに生成されます。

サポートされるブラウザのバージョン

- ・ Safariバージョン15.0(16612.1.29.41.4、16612)
 - ・ Safariバージョン13.0以前はサポートされなくなりました
- ・ Chromeバージョン94.0.4606.71(公式ビルド)(x86_64)
- ・ Firefoxバージョン92.0.1(64ビット)
- ・ Microsoft Edgeバージョン94.0.992.38(公式ビルド)(64ビット)
 - ・ Microsoft Edgeバージョン79以前はサポートされなくなりました

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:9.6-1.3
- ・ blackducksoftware/blackduck-authentication:2021.10.0
- ・ blackducksoftware/blackduck-webapp:2021.10.0
- ・ blackducksoftware/blackduck-scan:2021.10.0
- ・ blackducksoftware/blackduck-jobrunner:2021.10.0
- ・ blackducksoftware/blackduck-cfssl:1.0.4
- ・ blackducksoftware/blackduck-logstash:1.0.11
- ・ blackducksoftware/blackduck-registration:2021.10.0
- ・ blackducksoftware/blackduck-nginx:2.0.9
- ・ blackducksoftware/blackduck-documentation:2021.10.0
- ・ blackducksoftware/blackduck-upload-cache:1.0.19
- ・ blackducksoftware/blackduck-redis:2021.10.0
- ・ blackducksoftware/blackduck-bomengine:2021.10.0
- ・ blackducksoftware/blackduck-matchengine:2021.10.0
- ・ blackducksoftware/blackduck-webui:2021.10.0

- sigsynopsys/bdba-worker:2021.9.1
- blackducksoftware/rabbitmq:1.2.5

APIの機能強化

GET /api/project-groupsの権限の修正

GET /api/project-groups apiエンドポイントには、次の修正が加えられています。

- GET api/project-groups ユーザーが検索結果として表示することを許可されているプロジェクトグループのみが返されます。
- GET api/project-groups/<project group ID> スーパーユーザーの役割を持つユーザーには「HTTP 200 OK」が返され、それ以外のユーザーには「HTTP 403 Forbidden」メッセージが返されます。

GET /api/users/{userId}の権限の変更

GET /api/users/{userId}エンドポイントでは、権限チェックが実行されなくなりました（以前はUSERMGMT_READチェックが必要でした）。

- GET /api/users/エンドポイント（全ユーザーをリスト）は、今後もUSERMGMT_READ権限で保護されます。
- /api/projects/{projectId} APIのprojectOwnerユーザー（ユーザーの権限ステータスに関係なく）は今後も提供されます。
- Black Duckバージョン2021.8.2でプロジェクトの役割に追加されたUSERMGMT_READ権限は削除されます。

GET /api/project-groupsの新しいフィルタパラメータ

特定のプロジェクトグループを検索するために、exactNameという新しいフィルタパラメータが追加されました。[真]の場合、exactName フィルタはqの名前値とマッチするプロジェクトグループのみを返します。プロジェクトグループの検索条件では、大文字と小文字は区別されません。マッチするグループがない場合は、何も返されません。また、exactName フィルタが[真]の場合は、qパラメータを指定する必要があります。指定しない場合は、プロジェクトグループは返されません。

/api/project-groupsリクエストでフィルタを使用する方法については、以下を参照してください。

```
/api/project-groups?q=name:<project group name>&filter=exactName:true
```

CPEサポートAPIの改善

次の3つの新しいパブリックAPIが追加されました。

- GET /api/cpes [searchParamは必須です。マッチするCPE IDが返されます]
- GET /api/cpes/{cpeId}/versions [CPE IDにマッチするコンポーネントバージョンが返されます]
- GET /api/cpes/{cpeId}/variants [CPE IDにマッチするコンポーネント取得元が返されます]

Copyright 2.0データおよび新しいレガシーエンドポイント

Black Duck は現在、新しい著作権データを提供するために、既存のエンドポイント（以下）を使用してCopyright 2.0データを展開しようとしています。削除または追加される応答フィールドはありません。

```
GET /api/components/{componentId}/versions/{componentVersionId}/origin/{originId}/file-copyrights
```

新しいエンドポイントを作成して、Copyright 1.0(akaレガシー)データを引き続き提供します。

```
GET /api/components/{componentId}/versions/{componentVersionId}/origin/{originId}/file-copyrights-legacy
```

注:この新しいエンドポイントは、Black Duck UIでは直接使用されず、パブリックAPIを介してのみ使用されます。また現在、既存のエンドポイントではCopyright 2.0データが返されるため、Black Duckのすべてのお客様(使用しているバージョンに関係なく)にこの新しいデータが表示されます。

パブリックAPIを使用したlastScanDateの公開

現在、以下のAPIはパブリックAPI応答でlastScanDateを公開しています。

```
GET /api/projects/{projectId}/versions/{projectVersionId}/bom-status
```

2021.10.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (HUB-29413)。[コンポーネントの追加]または[コンポーネントの編集]モダルでのコンポーネントの検索がより正確となり、カスタムコンポーネントを簡単に検索できるようになりました。
- ・ (HUB-26545およびHUB-30185)。次のPublic REST APIエンドポイントが、componentModification、componentModified、componentPurposeコンポーネントの条件を想定どおりに更新していなかった問題が修正されました。
 - ・ /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}
 - ・ /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}
- ・ (HUB-30474)。ユーザーが特定プロジェクトにアクセスできない場合、[影響を受けるプロジェクト]ページに表示されるカウントが実際の結果とマッチしていなかった問題が修正されました。
- ・ (HUB-30623)。クライアントが原因で多数のエラーが発生した場合、スタックトレースのログ記録によって大きなログファイルが生成されたり、実際よりも深刻なログレベルで誤ってエラーが記録されたりしていた問題が修正されました。
- ・ (HUB-30099)。既存の構成表で、KBの更新によって脆弱性ステータスが更新されなかった問題が修正されました。構成表コンポーネント - 現在のステータスがユーザー更新またはシステム更新ではない場合に、修正ステータスに変化すると、バージョン脆弱性修正(構成表 - セキュリティビューにある)は、KB更新ジョブによって更新されるようになりました。
- ・ (HUB-29773)。/api/projects/<project ID>/versions/<version ID>/vulnerable-bom-componentsエンドポイントの応答時間が想定よりも長くなっていた問題が修正されました。このリクエストには、バージョン構成表コンポーネントごとに1つのライセンス定義のみが含まれるようになりました。この変更により、応答時間が短縮されました。ライセンスの上書きでProtex構成表をインポートした場合は、表示される結果の件数が少なくなっています。
- ・ (HUB-26924)。SAML SSOユーザーがログインに失敗したときに、ユーザーフレンドリーなエラーメッセージが表示されるように修正されました。SSO構成が間違っている場合は、構成の問題を通知するためにエラーページが表示されます。HUBでユーザーが無効になっている場合は、エラーページが表示され、ユーザーはシステム管理者に連絡するか、未許可のページにアクセスするように指示されます。
- ・ (HUB-31176)。修正ステータスが特定のプロジェクトバージョンに関連付けられている場合、高速スキャンポリシー評価で構成表ステータスがチェックされていなかった問題が修正されました。
- ・ (HUB-30808)。プロジェクトの構成表でコンポーネントの「追加フィールド」をレビューする場合、カスタムフィールド管理の[構成表コンポーネント]タブで作成されたカスタムフィールドが返されていなかった問題が修正されました。構成表コンポーネントのカスタムフィールドを編集する場合、最大100個のカスタムフィールドが表示されます。
- ・ (HUB-30922)。プロジェクトバージョンレベルの説明が表示されなかった問題が修正されました。現在、このフィールドには、プロジェクトレベルで使用する説明が表示されるようになりました。
- ・ (HUB-31482)。HUB 2021.6.2以降、[スニペット確認]ページにライセンスが表示されていなかった問題が修正されました。

- ・ (HUB-31003)。脆弱性を一括で修復しようとする、「HTTP 500 Internal Server Error」が発生していた問題が修正されました。
- ・ (HUB-31425)。バージョン詳細レポートで、以前のバージョンのHUBと比較してクエリを実行/完了するまでに長時間を要していた問題が修正されました。
- ・ (HUB-29598)。コンポーネントページの[印刷]ボタンで生成したPDFでは、バーが長くなり過ぎて脆弱性の件数が押し出されて表示されない可能性があった問題が修正されました。
- ・ (HUB-30133)。Helm導入環境のTシャツのサイズ設定yamlファイルにあるwebuiコンテナで、XL導入用のメモリがLよりも小さくなっていた問題が修正されました。webuiコンテナのメモリ制限は、x-large.yaml tshirtサイズで1024 Miに引き上げられました。
- ・ (HUB-28889)。RabbitMQにアクセスできない場合、構成表エンジンが起動できない可能性があった問題が修正されました。
- ・ (HUB-30215)。BDSA-2020-1311で回避策があるという誤った報告が行われていた問題が修正されました。
- ・ (HUB-30857)。[影響を受けるプロジェクト]ページの脆弱性について、表示される項目では、無視されるコンポーネントからの脆弱性の件数が除外されていたが、項目の総合計数を確認するとその数値が含まれていたというバグが修正されました。現在では、項目の総数からも、無視されるコンポーネントの脆弱性件数は除外されています。
- ・ (HUB-30603)。プロジェクトの[セキュリティ]タブで、BDSAまたはCVEレコードの下にあるコメントがグレー表示になっていたとしても、ユーザーはコメントの内容をすべて確認できたという問題が修正されました。
- ・ (HUB-28753)。Dockerで作成された場合、BomEngineはHUB_PROXY_PASSWORD_FILEシークレット値を受け入れず、407 AUTHENTICATION REQUIREDエラーを返していた問題が修正されました。
- ・ (HUB-31483)。日本語ローカライゼーションの場合、[ポリシー違反]モーダルで、ポリシー上書き日とユーザー情報が誤って表示されていた問題が修正されました。

Black Duck 2021.8.x

バージョン2021.8.8の新機能および変更された機能

Black Duck バージョン2021.8.8はメンテナンスリリースであり、新機能や変更された機能はありません。認証されていないリモート攻撃者がクロスサイトスクリプティング攻撃を実行できるようになる[CVE-2022-30278](#)に対処するために、オンラインヘルプを修正しました。

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:9.6-1.1
- ・ blackducksoftware/blackduck-authentication:2021.8.8
- ・ blackducksoftware/blackduck-webapp:2021.8.8
- ・ blackducksoftware/blackduck-scan:2021.8.8
- ・ blackducksoftware/blackduck-jobrunner:2021.8.8
- ・ blackducksoftware/blackduck-cfssl:1.0.3
- ・ blackducksoftware/blackduck-logstash:1.0.15
- ・ blackducksoftware/blackduck-registration:2021.8.8
- ・ blackducksoftware/blackduck-nginx:2.0.6
- ・ blackducksoftware/blackduck-documentation:2021.8.8

- `blackducksoftware/blackduck-upload-cache:1.0.18`
- `blackducksoftware/blackduck-redis:2021.8.8`
- `blackducksoftware/blackduck-bomengine:2021.8.8`
- `blackducksoftware/blackduck-matchengine:2021.8.8`
- `blackducksoftware/blackduck-webui:2021.8.8`
- `sigsynopsys/bdba-worker:2021.7.0`
- `blackducksoftware/rabbitmq:1.2.3`

2021.8.8で修正された問題

お客様から報告された次の問題が修正されました。

- (HUB-32811)。JDBCのパラメータが多すぎた結果としてプロジェクトバージョンのVersionReportJobが失敗することにより、一部のレポートが生成できない可能性があった問題が修正されました。

バージョン2021.8.7の発表

Apache Log4j2のセキュリティアドバイザリ(CVE-2021-45046およびCVE-2021-45105)

Apache Organizationは、Log4j2コンポーネントの新しいバージョン(2.17.0)をリリースしました。これは、バージョン2.15.0および2.16.0で修正されていない追加の脆弱性に対処するものです。

[CVE-2021-45046](#)では、コンテキストルックアップまたはスレッドコンテキストマップパターンのいずれかを使用するデフォルト以外のパターンレイアウトが、ログ構成で使用されているときに、攻撃者がスレッドコンテキストマップ(MDC)入力データを制御して、JNDIルックアップパターンを使った悪意のある入力データを作成することができ、その結果サービス拒否(DOS)攻撃が引き起こされます。

[CVE-2021-45105](#)では、攻撃者がスレッドコンテキストマップ(MDC)入力データを制御して、再帰的なルックアップを含む悪意のある入力データを作成でき、その結果、プロセスを終了させるStackOverflowErrorが発生し、サービス拒否(DOS)攻撃が引き起こされます。

詳細については、[ApacheのLog4jセキュリティ脆弱性のページ](#)を参照してください。

Black Duck 2021.8.6バージョンで述べられているように、Black Duckの製品、サービス、システムに対する露出は限定的であると考えられます。露出があった範囲に対しては、状況を修正済みであるか、または修正の過程にあります。今後の更新については、[コミュニティページ](#)を引き続きご確認ください。

バージョン2021.8.7の新機能および変更された機能

Log4jの更新

Apache Log4j 2 Javaライブラリは、重要なCVE-2021-45046およびCVE-2021-45105の脆弱性に対処するために2.17.0に更新されました。

Logstashの更新

Black Duckで使用するLogstashイメージは、Log4j2バージョン2.17.0を使用する7.16.2にアップグレードされました。

コンテナバージョン

- `blackducksoftware/blackduck-postgres:9.6-1.1`
- `blackducksoftware/blackduck-authentication:2021.8.7`
- `blackducksoftware/blackduck-webapp:2021.8.7`

- ・ blackducksoftware/blackduck-scan:2021.8.7
- ・ blackducksoftware/blackduck-jobrunner:2021.8.7
- ・ blackducksoftware/blackduck-cfssl:1.0.3
- ・ blackducksoftware/blackduck-logstash:1.0.15
- ・ blackducksoftware/blackduck-registration:2021.8.7
- ・ blackducksoftware/blackduck-nginx:2.0.6
- ・ blackducksoftware/blackduck-documentation:2021.8.7
- ・ blackducksoftware/blackduck-upload-cache:1.0.18
- ・ blackducksoftware/blackduck-redis:2021.8.7
- ・ blackducksoftware/blackduck-bomengine:2021.8.7
- ・ blackducksoftware/blackduck-matchengine:2021.8.7
- ・ blackducksoftware/blackduck-webui:2021.8.7
- ・ sigsynopsys/bdba-worker:2021.7.0
- ・ blackducksoftware/rabbitmq:1.2.3

2021.8.7で修正された問題

次の問題が修正されました。

- ・ (HUB-32233)。CVE-2021-45046およびCVE-2021-45105に対応して、Log4jをバージョン2.17.0にアップグレードしました。
- ・ (HUB-32295)。Bitnami LogstashをLog4j 2.17.0を使用する7.16.2バージョンに更新しました。

バージョン2021.8.6の発表

Apache Log4J2のセキュリティアドバイザリ(CVE-2021-44228)

Black Duck は、プロジェクトのGitHubを介して2021年12月9日に公開された、Log4Shell(またはLogJam)と呼ばれるオープンソースのApache Log4j 2 Javaライブラリに関連するセキュリティの問題を認識しています。この脆弱性により、認証されていないリモートコードの実行が可能になり、Apache Log4j 2バージョン2.0~2.14.1に影響が及んでいます。詳細については、[CVEの公式投稿](#)を参照してください。

現時点でわかっている知見に基づいて、Black Duckの製品、サービス、システムに対する露出は限定的であると考えています。露出があった範囲に対しては、状況を修正済みであるか、または修正の過程にあります。今後の更新については、コミュニティページを引き続きご確認ください。

<https://www.synopsys.com/blogs/software-security/zero-day-exploit-log4j-analysis/>も参照してください。

バージョン2021.8.6の新機能および変更された機能

Log4jの更新

Apache Log4j 2 Javaライブラリは、重要なCVE-2021-44228の脆弱性に対処するために2.15.0に更新されました。

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:9.6-1.1
- ・ blackducksoftware/blackduck-authentication:2021.8.6

- blackducksoftware/blackduck-webapp:2021.8.6
- blackducksoftware/blackduck-scan:2021.8.6
- blackducksoftware/blackduck-jobrunner:2021.8.6
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash:1.0.13
- blackducksoftware/blackduck-registration:2021.8.6
- blackducksoftware/blackduck-nginx:2.0.6
- blackducksoftware/blackduck-documentation:2021.8.6
- blackducksoftware/blackduck-upload-cache:1.0.18
- blackducksoftware/blackduck-redis:2021.8.6
- blackducksoftware/blackduck-bomengine:2021.8.6
- blackducksoftware/blackduck-matchengine:2021.8.6
- blackducksoftware/blackduck-webui:2021.8.6
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

2021.8.6で修正された問題

次の問題が修正されました。

- (HUB-32174)。CVE-2021-44228に対応して、Log4jをバージョン2.15.0にアップグレードしました。

バージョン2021.8.5の新機能および変更された機能

Black Duck バージョン2021.8.5はメンテナンスリリースであり、新機能や変更された機能はありません。

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.8.5
- blackducksoftware/blackduck-webapp:2021.8.5
- blackducksoftware/blackduck-scan:2021.8.5
- blackducksoftware/blackduck-jobrunner:2021.8.5
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash:1.0.10
- blackducksoftware/blackduck-registration:2021.8.5
- blackducksoftware/blackduck-nginx:2.0.6
- blackducksoftware/blackduck-documentation:2021.8.5
- blackducksoftware/blackduck-upload-cache:1.0.18
- blackducksoftware/blackduck-redis:2021.8.5
- blackducksoftware/blackduck-bomengine:2021.8.5

- ・ blackducksoftware/blackduck-matchengine:2021.8.5
- ・ blackducksoftware/blackduck-webui:2021.8.5
- ・ sigsynopsys/bdba-worker:2021.7.0
- ・ blackducksoftware/rabbitmq:1.2.3

2021.8.5で修正された問題

- ・ (HUB-31482)。Black Duckバージョン2021.6.2以降、[スニペット確認]ページにライセンスが表示されていなかった問題が修正されました。
- ・ (HUB-31663)。QuartzSearchDashboardRefreshJobが、ジョブの複数インスタンスをスケジュールしようとして、ブロックされたクエリが大量に発生していた問題が修正されました。

バージョン2021.8.4の新機能および変更された機能

Black Duck バージョン2021.8.4はメンテナンスリリースであり、新機能や変更された機能はありません。

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:9.6-1.1
- ・ blackducksoftware/blackduck-authentication:2021.8.4
- ・ blackducksoftware/blackduck-webapp:2021.8.4
- ・ blackducksoftware/blackduck-scan:2021.8.4
- ・ blackducksoftware/blackduck-jobrunner:2021.8.4
- ・ blackducksoftware/blackduck-cfssl:1.0.3
- ・ blackducksoftware/blackduck-logstash:1.0.10
- ・ blackducksoftware/blackduck-registration:2021.8.4
- ・ blackducksoftware/blackduck-nginx:2.0.6
- ・ blackducksoftware/blackduck-documentation:2021.8.4
- ・ blackducksoftware/blackduck-upload-cache:1.0.18
- ・ blackducksoftware/blackduck-redis:2021.8.4
- ・ blackducksoftware/blackduck-bomengine:2021.8.4
- ・ blackducksoftware/blackduck-matchengine:2021.8.4
- ・ blackducksoftware/blackduck-webui:2021.8.4
- ・ sigsynopsys/bdba-worker:2021.7.0
- ・ blackducksoftware/rabbitmq:1.2.3

2021.8.4で修正された問題

- ・ (HUB-31425)。バージョン詳細レポートで、以前のバージョンのHUBと比較してクエリを実行/完了するまでに長時間を要していた問題が修正されました。

バージョン2021.8.3の新機能および変更された機能

レポートデータベースの機能強化

次のデータをレポートスキーマの下でscan_stats_viewに追加しました。

- scan_size

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.8.3
- blackducksoftware/blackduck-webapp:2021.8.3
- blackducksoftware/blackduck-scan:2021.8.3
- blackducksoftware/blackduck-jobrunner:2021.8.3
- blackducksoftware/blackduck-cfssl:1.0.3
- blackducksoftware/blackduck-logstash:1.0.10
- blackducksoftware/blackduck-registration:2021.8.3
- blackducksoftware/blackduck-nginx:2.0.6
- blackducksoftware/blackduck-documentation:2021.8.3
- blackducksoftware/blackduck-upload-cache:1.0.18
- blackducksoftware/blackduck-redis:2021.8.3
- blackducksoftware/blackduck-bomengine:2021.8.3
- blackducksoftware/blackduck-matchengine:2021.8.3
- blackducksoftware/blackduck-webui:2021.8.3
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

2021.8.3で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-29959、HUB-30391、HUB-30397)。構成表の準備中にナレッジベースからの「500 内部エラー」応答によりスキャンが完了しない可能性があった問題が修正されました。
- (HUB-31047)。バージョン構成表コンポーネントページを表示する際、UIがバックエンドの呼び出しを重複して行っており、データベースに不要な負荷がかかっていた問題が修正されました。
- (HUB-30074)。アップロードソース情報が更新される前に、非常に小さなコードの場所のスニペットスキャンが終了する場合があります、アップロードされたソースが失われたように見えていた問題が修正されました。

バージョン2021.8.2の新機能および変更された機能

Black Duck バージョン2021.8.2はメンテナンスリリースであり、新機能や変更された機能はありません。

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.1

- `blackducksoftware/blackduck-authentication:2021.8.2`
- `blackducksoftware/blackduck-webapp:2021.8.2`
- `blackducksoftware/blackduck-scan:2021.8.2`
- `blackducksoftware/blackduck-jobrunner:2021.8.2`
- `blackducksoftware/blackduck-cfssl:1.0.3`
- `blackducksoftware/blackduck-logstash:1.0.10`
- `blackducksoftware/blackduck-registration:2021.8.2`
- `blackducksoftware/blackduck-nginx:2.0.6`
- `blackducksoftware/blackduck-documentation:2021.8.2`
- `blackducksoftware/blackduck-upload-cache:1.0.18`
- `blackducksoftware/blackduck-redis:2021.8.2`
- `blackducksoftware/blackduck-bomengine:2021.8.2`
- `blackducksoftware/blackduck-matchengine:2021.8.2`
- `blackducksoftware/blackduck-webui:2021.8.2`
- `sigsynopsys/bdba-worker:2021.7.0`
- `blackducksoftware/rabbitmq:1.2.3`

2021.8.2で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-31078)。Kubernetesの環境で、Black Duck 2021.8のインストールまたはアップグレードの一部として`--reuse-values`フラグを使用すると、インストールまたはアップグレードが正常に終了しませんでした。その問題は文書化されました。詳細については、Helmチャートの下にあるREADME.mdを参照してください。
- (HUB-31086)。いくつかのプロジェクトバージョンで、[構成表]ページの右上にあるスニペットボックスが欠落していた問題が修正されました。
- (HUB-31156)。プロジェクトレベルで構成表マネージャのロールを持っていて、グローバルなロールや全般的なロールは持っていないユーザーが、プロジェクト構成表にアクセスできなかった問題が修正されました。

バージョン2021.8.1の新機能および変更された機能

Black Duck バージョン2021.8.1はメンテナンスリリースであり、新機能や変更された機能はありません。

コンテナバージョン

- `blackducksoftware/blackduck-postgres:9.6-1.1`
- `blackducksoftware/blackduck-authentication:2021.8.1`
- `blackducksoftware/blackduck-webapp:2021.8.1`
- `blackducksoftware/blackduck-scan:2021.8.1`
- `blackducksoftware/blackduck-jobrunner:2021.8.1`
- `blackducksoftware/blackduck-cfssl:1.0.3`
- `blackducksoftware/blackduck-logstash:1.0.10`
- `blackducksoftware/blackduck-registration:2021.8.1`

- blackducksoftware/blackduck-nginx:2.0.6
- blackducksoftware/blackduck-documentation:2021.8.1
- blackducksoftware/blackduck-upload-cache:1.0.18
- blackducksoftware/blackduck-redis:2021.8.1
- blackducksoftware/blackduck-bomengine:2021.8.1
- blackducksoftware/blackduck-matchengine:2021.8.1
- blackducksoftware/blackduck-webui:2021.8.1
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

2021.8.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-31029)。個人/グループのスーパーユーザーのロールが、プロジェクトマネージャのロール設定で上書きされていた問題が修正されました。
- (HUB-30808)。プロジェクトの構成表でコンポーネントの「追加フィールド」をレビューする場合、カスタムフィールド管理の[構成表コンポーネント]タブで作成されたカスタムフィールドが返されていなかった問題が修正されました。
- (HUB-30655)。スーパーユーザーのロールを持たないユーザーが、[管理]メニューの[プロジェクトグループ管理]オプションを表示できていた問題が修正されました。
- (HUB-31077)。Helmチャートのプロパティに変更が加えられたため、Kubernetesの導入環境では、Black Duck HUB 2021.6.0を2021.8.xにアップグレードできない可能性があった問題が修正されました。他の旧バージョンには影響はありません。

バージョン2021.8.0の発表

Black Duck 2021.8.0リリースに必要なDetect 7.4

Black Duck バージョン2021.8.0を実行するには、Detect 7.4が必要です。アップグレードする際には、この最小バージョン要件を満たしていることを確認してください。

CentOS-7上のDesktop Scanner

依存関係が更新されたため、最新バージョンのDesktop ScannerはCentOS-7では実行されません。そのため、古いバージョンのElectron 12で動作するCentOS-7ビルド専用に関別のRPMが作成されました。Electron 12がサポートされている限り、この個別のCentOS-7ビルドを維持します。

現在のダウンロードに加えて、ツールページにCentOS-7ダウンロード専用のリンクが追加されました。通常のRPM、Debianパッケージ、macOSおよびWindowsインストーラが利用できます。

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.6.0が日本語にローカライズされました。

簡体字中国語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.2.0が簡体字中国語にローカライズされました。

廃止されたAPI

次のエンドポイントは削除されました。

- GET /api/scan/{scanId}/bom-entries

以下の廃止されたエンドポイントは「410 GONE」エラーを返し、ターゲットリソースへのアクセスが利用できなくなったことを示します。

- GET /oauthclients
- POST /oauthclients
- DELETE /oauthclients/{oauthClientId}
- GET /oauthclients/{oauthClientId}
- PUT /oauthclients/{oauthClientId}
- POST /vulnerabilities/vulndb-copy

バージョン2021.8.0の新機能および変更された機能

PostgreSQL 13の外部データベースのサポート

Black Duck は、外部PostgreSQLを使用する新規インストール用にPostgreSQL 13をサポート・推奨するようになりました。2021.8.xへの移行では、PostgreSQL 13への移行は必要ありません。

内部PostgreSQLコンテナのユーザーは、アクションは必要ありません。

PostgreSQL 12はサポートされていません。

インストールマニュアルは、今後のリリースで更新される予定です。

Azureをご利用のお客様へのお知らせ

Azure PostgreSQL 13でのBlack Duckのサポートは、Azure PostgreSQL 13のフル リリースまでは可能な範囲での最善のサポートの提供となり、問題の解決は保証されません。したがって、本番環境への導入にAzure PostgreSQL 13を使用しないことを強くお勧めします。Azure PostgreSQL 11を使用する必要があります。

PostgreSQL 13のAzureサポートの詳細については、<https://docs.microsoft.com/en-us/azure/postgresql/concepts-version-policy>を参照してください。


スキャンの新しいシステム設定: コンポーネント依存関係の重複感度

この設定では、スキャン中に検出されたコンポーネントの重複パッケージIDを[ソース]ページに表示する方法を変更できます。以前のリリースおよび2021.8.0のデフォルト設定(1に設定)では、スキャン中の検出頻度に関係なく、1つのパッケージIDのみが[ソース]ページに表示されます。この設定を1より大きい値に変更すると、より多くのエントリが表示されるため、レイヤーごとの洞察が深まり、各コンポーネントがどのレイヤーから発生したかを判断することができます。この機能は、[構成表集約を使用して検出]を有効にしてスキャンし、1つのスキャンに集約されたさまざまなモジュールにおけるパッケージID参照を表示する場合に特に便利です。

スキャンの新しいシステム設定: 最小スキャン間隔

この設定では、LCAの強化された署名スキャンを使用するときに、特定のコードの場所に対して署名スキャンを実行できる最小時間間隔を変更できます。デフォルト設定は0、または最小スキャン間隔が設定されていないため、頻度に関係なくスキャンが実行されます。0より大きい値に設定すると、設定されたスキャン間隔より前に署名スキャンが実行された場合、スキャンは処理されません。たとえば4に設定すると、4時間が経過するまで署名の再スキャンが許可されません。この設定は、[管理]>[システム設定]>[スキャン]ページでグローバルに設定するか、Detectクライアントのコマンドラインオプションを使用して設定できます。注: この設定は、パラメーター

`detect.blackduck.signature.scanner.arguments='--signature-generation'`を使用してスキャンした場合にのみ使用されます。

 注：この機能を有効にすると、スキャン間隔が原因で署名スキャンが実行されなかった場合でも、Detectを使用した署名スキャンは成功ステータスで終了します。スキャンが実行されなかったことを示す警告メッセージがログに表示されますが、他の情報は表示されません。

高速スキャンのポリシー適用の変更

高速スキャンユーザーは、フルスキャン(従来)、高速スキャン、またはその両方の結果にポリシーを適用する方法を設定できるようになりました。バージョン2021.8.0以降のBlack Duck新規インストールのデフォルト設定は、フルスキャンにのみ適用されるように設定されます。高速スキャンを使用して、ポリシーに関係なくすべての脆弱性を検出するには、1つのポリシーを作成し、条件の重大度を0以上に設定します。

実行された高速スキャン数の自動累積カウントの追加

このカウントは正確であり、データが失われることはありませんが、一部のスキャンが後続日のデータから取得されるタイミングの問題がある場合があります。

高速スキャンの脆弱性条件のポリシー管理への追加

ポリシー管理では、次の脆弱性の条件が利用可能になりました。

- ・ CWE ID
- ・ ソリューションが利用可能
- ・ 回避策が利用可能
- ・ 攻撃が利用可能
- ・ ソースから到達可能
- ・ 修正ステータス

プロジェクトグループ管理

Black Duck は、Hub内のすべてのプロジェクトを論理的にグループ化します。これにより、どのプロジェクトがどの事業単位に属しているかを整理できるため、組織全体のリスクを簡単に確認できるようになりました。プロジェクトグループには、プロジェクトと他のプロジェクトグループの両方を含めることができ、マルチレベルの階層を提供できます。

ユーザーとグループは、任意の数の役割を持つプロジェクトグループに割り当てることができます。この割り当てにより、割り当てが下位レベルで明示的に上書きされない限り、指定された役割を持つグループの下プロジェクトにアクセスできるようになります。この概念により、まだ作成されていないプロジェクトへのデフォルトアクセス権をユーザーに設定できます。

さらに、検索ダッシュボードが拡張され、ユーザーがプロジェクトグループを介してアクセスできるプロジェクトの検索結果が返されるようになりました。

新しいユーザーの役割であるグローバルリリース作成者とプロジェクトグループ構成表アノテーター、および既存の役割への変更

プロジェクト作成者とグローバルコードスキャナという役割が持っていたグローバルリリース作成のアクセス権が取り消され、所有していない、またはアクセス権を持っていないプロジェクトのリリースを作成できなくなりました。この機能に依存しているユーザーのギャップを埋めるために、グローバルリリース作成者という新しい役割が追加されました。プロジェクト作成者やグローバルコードスキャナを使用している現在のすべてのユーザーは、アップグレード移行スクリプトの一部としてこの役割を自動的に継承します。つまり、この変更は、より狭いセキュリティの変更を利用したいと考えている現在のユーザーのためのものです。

プロジェクトグループ構成表アノテーターには、割り当てられたプロジェクトグループ内のすべてのプロジェクトに対する構成表アノテーター権限があります。つまり、プロジェクトグループに関連付けられているプロジェクトのコメントの追加や編集、カスタムフィールドの編集ができます。

Protex BOMツールトークンアクセスサポートの強化

Protex BOMツールでは、BD_HUB_TOKEN環境変数をサポートして、ProtexからエクスポートされたJSONをHubにアップロードできるようになりました。トークンを設定するには、コマンドプロンプトを使用して「-T」を追加します。

BD_HUB_TOKEN=[insert token here]変数を.bash_profileに追加して、変更を永続的にします。

脆弱性の通知の機能強化

新しい環境変数を追加しました: blackduck-config.evファイル内のBLACKDUCK_NOTIFY_WHEN_REMEDIATEDデフォルトはtrueですが、falseに設定すると、Black Duckでは「無視、修復完了、緩和、またはパッチ適用済み」の修正ステータスを持つ脆弱性に対する「新しい」脆弱性通知を送信も作成もできなくなります。

署名スキャンタイムアウトメッセージの拡張

署名スキャン中のネットワークタイムアウト(HUBからの応答を待機中)では、I/Oエラーではなくネットワークタイムアウトを示す正確なエラーメッセージ(コード74)が返されるようになりました。新しいメッセージ形式Scan <Corresponding Scan ID> failed: [<Reason why it happened and whether to contact an administrator or retry the scan>]が表示されます。

Black Duck Hubの再試行要求メカニズムの機能強化

ウェイターが導入され、HTTP 502/503/504応答を受信したときにスキャンのHubへのアップロードが再試行されるようになりました。スキャンが失敗したことを通知する前に、30秒ごとに10分間再試行します。

[スキャン]ページの拡張機能

[作成]列が[スキャン]ページに新しく追加され、スキャンが作成された日時を確認できるようになりました。列に表示される日付により、[作成日]オプションを使用してスキャンをフィルタリングするときに日付を簡単に比較できます。

バージョンのないコンポーネントの表層ライセンスリスク情報

不明なバージョンのコンポーネントのデフォルトライセンスを決定するための新しいロジックが導入されました。これは、コンポーネントの上位1,000バージョンで表示される最大回数に基づく推定ライセンスです。これにより、バージョンを選択しなくてもライセンスリスクを計算できます。ただし、より正確な結果を得るには、これらのコンポーネントを確認し、手動でバージョンを指定することをお勧めします。

レポートデータベースの機能強化

次のデータをレポートスキーマの下にscan_stats_viewに追加しました。

- user_id
- project_id
- project_name
- version_id
- version_name
- scan_id
- scan_name
- code_location_id

- ・ code_location_name
- ・ scan_type
- ・ scan_status
- ・ scan_start_at
- ・ scan_end_at
- ・ scan_duration
- ・ scan_age
- ・ scan_archived_at
- ・ application_id

ポリシールール条件の機能強化

総合スコアのポリシールール脆弱性条件カテゴリに、新しいポリシー条件演算子が追加されました。ポリシールールを作成または編集するときに、[次の値以下]を選択できるようになりました。

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:9.6-1.1
- ・ blackducksoftware/blackduck-authentication:2021.8.0
- ・ blackducksoftware/blackduck-webapp:2021.8.0
- ・ blackducksoftware/blackduck-scan:2021.8.0
- ・ blackducksoftware/blackduck-jobrunner:2021.8.0
- ・ blackducksoftware/blackduck-cfssl:1.0.3
- ・ blackducksoftware/blackduck-logstash:1.0.10
- ・ blackducksoftware/blackduck-registration:2021.8.0
- ・ blackducksoftware/blackduck-nginx:2.0.5
- ・ blackducksoftware/blackduck-documentation:2021.8.0
- ・ blackducksoftware/blackduck-upload-cache:1.0.18
- ・ blackducksoftware/blackduck-redis:2021.8.0
- ・ blackducksoftware/blackduck-bomengine:2021.8.0
- ・ blackducksoftware/blackduck-matchengine:2021.8.0
- ・ blackducksoftware/blackduck-webui:2021.8.0
- ・ sigsynopsys/bdba-worker:2021.7.0
- ・ blackducksoftware/rabbitmq:1.2.3

APIの機能強化

- ・ スニペットマッチを一括確認/確認解除、一括無視/無視解除するための新しいAPIが追加されました。
 - ・ PUT /api/projects/{projectId}/versions/{versionId}/bulk-snippet-bom-entries Media Type: application/vnd.blackducksoftware.bill-of-materials-6+json

- ・ 次のAPIエンドポイントが更新され、ユーザーがプロジェクトグループメンバーシップを介してアクセスできるプロジェクトが考慮されるようになりました。クエリパラメータもnameからentityNameに変更され、応答内容と同等になりました。
 - ・ GET /api/users/{userId}/assignable-projects
 - ・ GET /api/users/{userId}/assignable-project-groups/
 - ・ GET /api/usergroups/{userGroupId}/assignable-projects
 - ・ GET /api/usergroups/{userGroupId}/assignable-project-groups

2021.8.0で修正された問題

- ・ (HUB-29341)。--include-filesフラグを使用してProtexから構成表をエクスポートし、Hubインスタンスにインポートすると、Javaヒープ領域エラーが発生していた問題が修正されました。
- ・ (HUB-29005)。構成表にまったく同名でUUIDが異なる2つのコンポーネントがある場合、フィルタAPI(/api/projects/projectId/versions/versionId/components-filters?filterKey=bomComponents)は名前によってそれらをグループ化するのではなく、IDとそのバージョン(存在する場合)に基づいて2つの独立したコンポーネントを返す必要があった問題が修正されました。
- ・ (HUB-29567)。「更新日時」(または2021.8.0では「最終設定更新日時」)のタイムスタンプが更新されても、[プロジェクトバージョン]>[詳細]のユーザー名で更新されない可能性があった問題が修正されました。「最終設定更新日時」タイムスタンプとユーザー名で更新されたタイムスタンプは、プロジェクトのバージョンの詳細が変更された場合にのみ更新されるようになりました。
- ・ (HUB-30139)。Protex BOMツールの問題が修正されました。--include-filesフラグを使用しているときに「Unmarshalling Error:Illegal character」が発生していました。
- ・ (HUB-12280)。bdioファイルのアップロード時に、「bdioツリー」の下層にある場合、プロジェクトとの関連性が表示されていなかった問題が修正されました。
- ・ (HUB-29481)。同じ名前で大文字が異なるライセンスが通知レポートから除外されていた問題が修正されました。
- ・ (HUB-30143)。Protex BOMツール2021.6.0が最新のJDK(11.0.11)で動作しなかった問題が修正されました。
- ・ (HUB-29274)。[構成表]ページに循環参照がある場合にVersionReportJobによってjobrunnerにメモリ不足の問題を発生させる可能性があった問題が修正されました。
- ・ (HUB-29381)。プロジェクトバージョンがコンポーネントとして追加されたときに([追加] > [プロジェクト]を使用)、コンポーネントエントリに無効な[運用リスク]レベルが表示される可能性があった問題が修正されました。
- ・ (HUB-30087)。バージョン名にマルチバイトの英数字が含まれている場合に、プロジェクトバージョンクエリでバージョンが見つからなかった問題が修正されました。
- ・ (HUB-23686)。ノードファイルに対してDetectを実行しているときに、署名スキャナがスタックする可能性があった問題が修正されました。
- ・ (HUB-25592)。コンポーネント(またはコンポーネントのバージョン)の調整が構成表から自動で削除されていた問題が修正されました。
- ・ (HUB-25552)。「マッチ」タイプの調整を含むコンポーネント(またはコンポーネントのバージョン)が構成表から自動で追加/削除されていた問題が修正されました。
- ・ (HUB-29196)。ポリシー違反ポップアップをクリックしても非表示にならず、マウスカーソルがポリシー違反シンボルからすばやく離れていた問題が修正されました。
- ・ (HUB-29573)。ポリシー違反モーダルの表示時にポリシールールの説明の改行が無視されていた問題が修正されました。

- ・ (HUB-30611)。データベース移行スクリプトで、数値のユーザー名がエラーを引き起こしていた問題が修正されました。
- ・ (HUB-26611)。Detectで集約を使用したときに、直接的/推移的な依存関係が正しく報告されていなかった問題が修正されました。この修正は、Detect 7.4を使用している場合にのみ解決され、Detectで新しいサブプロジェクトdetect.bom.aggregate.remediation.modeを使用する必要があることに注意してください。
- ・ (HUB-22379)。一部のインスタンスでプロジェクトのタグ付けとタグポリシーの設定に数時間かかる可能性があったパフォーマンスの問題が修正されました。
- ・ (HUB-30141)。サポートされていない「リンク」オプションを含むHub swarm docker-compose.ymlの問題が修正されました。
- ・ (HUB-29549)。アクセス権チェックにより生じていた、[構成表]ページのロードに関するパフォーマンスの問題が修正されました。

Black Duck 2021.6.x

バージョン2021.6.2の新機能および変更された機能

Black Duck バージョン2021.6.2はメンテナンスリリースであり、新機能や変更された機能はありません。

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:9.6-1.1
- ・ blackducksoftware/blackduck-authentication:2021.6.2
- ・ blackducksoftware/blackduck-webapp:2021.6.2
- ・ blackducksoftware/blackduck-scan:2021.6.2
- ・ blackducksoftware/blackduck-jobrunner:2021.6.2
- ・ blackducksoftware/blackduck-cfssl:1.0.2
- ・ blackducksoftware/blackduck-logstash:1.0.10
- ・ blackducksoftware/blackduck-registration:2021.6.2
- ・ blackducksoftware/blackduck-nginx:2.0.5
- ・ blackducksoftware/blackduck-documentation:2021.6.2
- ・ blackducksoftware/blackduck-upload-cache:1.0.17
- ・ blackducksoftware/blackduck-redis:2021.6.2
- ・ blackducksoftware/blackduck-bomengine:2021.6.2
- ・ blackducksoftware/blackduck-matchengine:2021.6.2
- ・ blackducksoftware/blackduck-webui:2021.6.2
- ・ sigsynopsys/bdba-worker:2021.06
- ・ blackducksoftware/rabbitmq:1.2.2

2021.6.2で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (HUB-30493)。NGINX構成でAlertのプロキシ証明書の場所を指定したことにより、ホストされたユーザーがBlackduck Alertインスタンスにアクセスできなかった問題が修正されました。

バージョン2021.6.1の新機能および変更された機能

Black Duck Security Advisory (BDSA) のリモート コード 実行 手順

Black Duck は、2021.6.1リリースにおいて、リモートでのコード実行(RCE)を可能にする脆弱性に注目しています。Black DuckのUIでは、BDSAの脆弱性にRCEタグがある場合、BDSAのフル レコード、脆弱性の表、特定のコンポーネントの[セキュリティ]タブに表示されます。

脆弱性APIは、bdsaTagsという名前の配列を使用して脆弱性を報告します。bdsaTag配列に「RCE」が含まれている場合、この脆弱性によりリモートでコードが実行される可能性があります。

- ・ /api/components/{componentId}/vulnerabilities
- ・ /api/components/{componentId}/versions/{componentVersionId}/vulnerabilities
- ・ /api/components/{componentId}/versions/{componentVersionId}/origin/{componentVersionOriginId}/vulnerabilities
- ・ /api/projects/{projectId}/versions/{versionId}/components/{componentId}/versions/{componentVersionId}/origins/{componentVersionOriginId}/vulnerabilities

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:9.6-1.1
- ・ blackducksoftware/blackduck-datadog:1.0.1
- ・ blackducksoftware/blackduck-solr:1.0.0
- ・ blackducksoftware/blackduck-authentication:2021.6.1
- ・ blackducksoftware/blackduck-webapp:2021.6.1
- ・ blackducksoftware/blackduck-scan:2021.6.1
- ・ blackducksoftware/blackduck-jobrunner:2021.6.1
- ・ blackducksoftware/blackduck-cfssl:1.0.2
- ・ blackducksoftware/blackduck-logstash:1.0.10
- ・ blackducksoftware/blackduck-registration:2021.6.1
- ・ blackducksoftware/blackduck-nginx:2.0.3
- ・ blackducksoftware/blackduck-documentation:2021.6.1
- ・ blackducksoftware/blackduck-upload-cache:1.0.17
- ・ blackducksoftware/blackduck-redis:2021.6.1
- ・ blackducksoftware/blackduck-bomengine:2021.6.1
- ・ blackducksoftware/blackduck-matchengine:2021.6.1
- ・ blackducksoftware/blackduck-webui:2021.6.1
- ・ sigsynopsys/bdba-worker:2021.06
- ・ blackducksoftware/rabbitmq:1.2.2

2021.6.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (HUB-29202)。2021.4.0のバイナリスキャンコンテナ(bdba-worker)が、タイムアウト値と再試行値を増やすとDocker Swarmで動作しなかった問題が修正されました。
- ・ (HUB-29405)。core_i7アーキテクチャの識別により、マッチが破棄されていた問題が修正されました。
- ・ (HUB-30134)。RabbitMQ接続の問題により、構成表エンジンが警告なしで起動に失敗していた問題が修正されました。
- ・ (HUB-30170)。デュアルスタックKubernetesを使用しているときに、Dockerエントリポイントの設定が正しくないためにRedisが起動しなかった問題が修正されました。
- ・ (HUB-30202)。[脆弱性の詳細]ページで、ユーザーがクリックしてBDSAスコアとNVDスコアを切り替えたときに、スコアメトリックの表示が正しく変更されていなかった問題が修正されました。

バージョン2021.6.0の発表

外部データベース用のPostgreSQLバージョン9.6のサポート終了

Black Duck 2021.6.0リリースの時点で、Black Duckは外部データベース用のPostgreSQLバージョン9.6のサポートを終了しました。

Black Duck は、外部データベース用のPostgreSQLバージョン11.xのみをサポートするようになりました。

廃止されたページ

以前にお知らせしたように、[スキャン] > [コンポーネント]ページは削除されました。

廃止されたAPI

次のエンドポイントは廃止されました。

- ・ GET /oauthclients
- ・ POST /oauthclients
- ・ DELETE /oauthclients/{oauthClientId}
- ・ GET /oauthclients/{oauthClientId}
- ・ PUT /oauthclients/{oauthClientId}
- ・ POST /vulnerabilities/vulndb-copy

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.4.0が日本語にローカライズされました。

バージョン2021.6.0の新機能および変更された機能

新しいコンテナとシステム要件の変更

2021.6.0リリースでは、次のようになります。

- ・ 新しいコンテナblackduck-webuiが追加され、Black Duckのパフォーマンスの向上、キャッシュ機能の向上、将来の拡張性が実現されました。


- ・ 高速スキャン機能は、すべてのBlack Duckのお客様が使用できるようになりました。この機能を使用するには、blackduck-matchengineという新しいコンテナが必要です。このコンテナは、Black Duck KnowledgeBaseへの接続を管理し、KnowledgeBaseの結果を短い間隔でキャッシュします。

以下は、すべてのコンテナの単一インスタンスの実行に必要な最小ハードウェアです。メモリ要件は、サポートする同時高速スキャンの数によって異なることに、注意してください。

- ・ 7 CPU
- ・ Redisの最小構成の場合は28.5 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は31.5 GB RAM。これにより、最大100の同時高速スキャンがサポートされます。
Redisの最小構成の場合は30 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は33 GB RAM。これにより、150以上の高速スキャンがサポートされますが、サポートされる高速スキャンの最大数は現在判定中です。
- ・ データベースおよびその他のBlack Duckコンテナ用に250 GBの空きディスク容量
- ・ データベースバックアップに適した容量

以下は、Black Duck – Binary AnalysisでBlack Duckを実行するために必要な最小ハードウェアです。

- ・ 8 CPU
- ・ Redisの最小構成の場合は32.5 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は35.5 GB RAM。これにより、最大100の同時高速スキャンがサポートされます。
Redisの最小構成の場合は34 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は37 GB RAM。これにより、150以上の高速スキャンがサポートされますが、サポートされる高速スキャンの最大数は現在判定中です。
- ・ データベースおよびその他のBlack Duckコンテナ用に350 GBの空きディスク容量
- ・ データベースバックアップに適した容量

 注：binaryscannerコンテナを1個追加することにより、1 CPU、2 GB RAM、100 GBの空きディスク容量の追加が必要になります。

高速スキャン

高速スキャンはすべてのお客様にご利用いただけます。

Black Duckの高速スキャンは、開発者が、プロジェクトに含まれているオープンソースコンポーネントのバージョンが、オープンソースの使用に関する企業ポリシーに違反しているかどうかを迅速に判断する方法を提供します。Black Duck Detectを使用すると、高速スキャンがパッケージマネージャのスキャンのみを使用し、Black Duckサーバーデータベースとやり取りしないので、迅速に結果が返されます。クイックフィードバックが必要な場合や、Black Duckでデータを保持する必要がない場合は、高速スキャンを使用します。

高速スキャンを使用すると、Black Duckの追加のインスタンスを展開しなくても、何千ものスキャンを実行できます。プロジェクトバージョンなしで、またはBlack Duckのユーザーインターフェイスにアクセスせずに使用できる、実用的な結果(ビルドの失敗など)を提供します。

新しいジョブサブシステム

ジョブサブシステムが新しい実装に置き換えられました。

- ・ ジョブのステータスには次のようなものがあります。
 - ・ 保留
 - ・ 進行中
 - ・ 完了
 - ・ エラー
- ・ 定期的またはオンデマンドのスケジュールに基づいてジョブをフィルタリングできます。

- ・ 新しい実装では、次のジョブが追加されました。
 - ・ BomAggregatePurgeOrphansCheckJob: 構成表データがプロジェクトバージョンに関連付けられていないかどうかを確認し、必要なジョブを開始します。
 - ・ BomVulnerabilityDataRecomputationCheckJob: 特定の設定が変更されたときに構成表の計算が必要かどうかをチェックし、必要なジョブを開始します。
 - ・ BomVulnerabilityDataRecomputationJob: ナレッジベースから受信したコンポーネント情報を更新します。
 - ・ HierarchicalVersionBomCheckJob: 階層的な構成表計算が必要かどうかをチェックし、その処理に必要なジョブを開始します。
 - ・ JobHistoryStatsJob-Calculate Daily Statistics: ジョブアクティビティに基づいて日次統計を計算します。
 - ・ JobHistoryStatsJob-Calculate Five Minute Statistics: ジョブアクティビティに基づいて、5分間隔で統計情報を計算します。
 - ・ JobHistoryStatsJob-Calculate Hourly Statistics: ジョブアクティビティに基づいて、1時間の統計情報を計算します。
 - ・ JobHistoryStatsJob-Prune Job History: 保持設定に基づいて、ジョブ履歴から古いレコードをプルーニングします。
 - ・ KbUpdateCheckJob: ナレッジベースから受信した更新を開始します。
 - ・ KbUpdateWorkflowJob-BDSA Vulnerability Update: ナレッジベースから受信したBDSAの脆弱性情報を更新します。
 - ・ KbUpdateWorkflowJob-Component Update: ナレッジベースから受信したコンポーネント情報を更新します。
 - ・ KbUpdateWorkflowJob-Component Version Update: ナレッジベースから受信したコンポーネントバージョンの更新を処理します。
 - ・ KbUpdateWorkflowJob-License Update: ナレッジベースから受信したライセンス情報を更新します。
 - ・ KbUpdateWorkflowJob-NVD Vulnerability Update: KnowledgeBaseから受信したNVD脆弱性情報を更新します。
 - ・ KbUpdateWorkflowJob-Summary: 最新のナレッジベース更新に関するサマリーレポートを発行します。
 - ・ LicenseTermFulfillmentCheckJob: ライセンスの履行処理が必要かどうかを確認し、必要なジョブを開始します。
 - ・ NotificationPurgeCheckJob: クリーンアップが必要な通知があるかどうかを確認し、必要なジョブを開始します。
 - ・ QuartzVersionBomEventCleanupJob: 保持ポリシーに基づいて構成表イベントをクリーンアップします。
 - ・ VersionBomComputationCheckJob: 構成表の計算が必要かどうかをチェックし、必要なジョブを開始して処理します。
 - ・ VersionBomNotificationCheckJob: 構成表計算結果の通知を発行します。
 - ・ WatchdogJob: 定期的なジョブを監視して正常に実行されていることを確認し、問題があると判断されたジョブの報告または修正を行います。
- ・ 次のジョブは削除されました。
 - ・ KbUpdateJob

レポートの機能強化

- ・ 新しいプロジェクトバージョンレポートlicense_conflicts_date_time.csvが追加されました。このプロジェクトバージョンのライセンス競合を一覧表示します。このレポートには、次のカラムがあります。
 - ・ コンポーネントID
 - ・ バージョンID
 - ・ コンポーネント名
 - ・ コンポーネントバージョン名
 - ・ 使用法
 - ・ ライセンスID
 - ・ ライセンス名
 - ・ ソース/タイプ
 - ・ ライセンス条項の責任
 - ・ ライセンス条項のカテゴリ
 - ・ ライセンス条項名
 - ・ 説明
 - ・ 競合ライセンスID
 - ・ 競合ライセンス名
 - ・ 競合ライセンス条項のソースタイプ
 - ・ 競合ライセンス条項の責任
 - ・ 競合ライセンス条項のカテゴリ
 - ・ 競合ライセンス条項名
 - ・ 競合ライセンス条項の説明
- ・ components_date_time.csvプロジェクトバージョンレポートの末尾に、新しい列[ライセンス競合あり]が追加されました。この列は、このコンポーネントバージョンにライセンス競合があるかどうかを示します。
- ・ レポートのファイル名では、UTCではなくシステムタイムゾーンが使用されるようになりました。

Black Duck KnowledgeBaseの著作権情報を更新する機能

Black Duck では、コンポーネントの取得元に関して、更新されたBlack Duck KnowledgeBase著作権情報を表示できるようになりました。新しいデータまたは更新されたデータがある場合、Black Duckは表示情報を更新しますが、編集内容は保持されます。

新しい役割

BOM Annotatorという新しいロールがBlack Duckに追加されました。この役割を持つユーザーは、プロジェクトへの読み取り専用アクセス権を持ち、構成表のコメントの追加または編集、構成表カスタムフィールドの更新を実行できます。

LDAPまたはSAMLグループの同期

Black DuckにLDAPまたはSAMLを設定するときにグループ同期を有効にすると、外部認証システム(LDAPまたはSSO)内のこのグループの名前が、[グループ名]ページの[外部グループ名]フィールドに表示されるようになります。

た。これで、外部システムでグループ名が変更された場合は、そのグループ名を編集して、外部認証システムのグループ名とBlack Duckのグループ名を同期させられるようになりました。

必須カスタムフィールドの強制

Black Duck では、必須カスタムフィールドを持つオブジェクトを編集する際にユーザーが値を入力する必要があるオプションが用意されました。

プロジェクト検索用の新しいフィルタ

Black Duck では、プロジェクトの検索時に次のフィルタを新しく提供します。

- ・ スキャンなし: このフィルタは、スキャンの一部になったことがないプロジェクトバージョンをすべて検索します。
- ・ スキャンされていない期間: このフィルタは、選択した期間以降にスキャンされていないプロジェクトバージョンをすべて検索します。

マップされていないコードの場所の保存期間

マップされていないコードの場所のデフォルト保存期間が365日から30日に変更されました。

[コンポーネントの追加/編集]ダイアログボックスの追加情報

使用するコンポーネントをより簡単に判別できるように、[コンポーネントの追加/編集]ダイアログボックスに、コンポーネントのホームページURLと、このコンポーネントを使用するプロジェクトバージョン番号が表示されるようになりました。

ポリシーの機能強化

次のコンポーネント条件には、「偽」オプションが含まれるようになりました。

- ・ プロジェクトバージョンとのライセンス競合
- ・ 未履行のライセンス条項
- ・ 不明なコンポーネントバージョン

C/C++マッチングの改善

2021.6.0リリースでは、LinuxドメインでC/C++をスキャンするお客様の構成表精度が向上しています。

新しいマッチタイプ

2021.6.0リリースでは、2つの新しいマッチタイプが追加されました。

- ・ 直接的な依存関係バイナリ: スキャンにより、使用中のバイナリに直接的な依存関係があると判定されました。
- ・ 推移的な依存関係バイナリ: スキャンにより、使用中のバイナリに推移的な依存関係があると判定されました。

サポートされるブラウザのバージョン

- ・ Safariバージョン14.0.3(15610.4.3.1.7、15610)
- ・ Chromeバージョン90.0.4430.72(公式ビルド)(x86_64)
- ・ Firefoxバージョン88.0(64ビット)
- ・ Microsoft Edgeバージョン90.0.818.41(公式ビルド)(64ビット)

コンテナバージョン

- blackducksoftware/blackduck-postgres:9.6-1.1
- blackducksoftware/blackduck-authentication:2021.6.0
- blackducksoftware/blackduck-webapp:2021.6.0
- blackducksoftware/blackduck-scan:2021.6.0
- blackducksoftware/blackduck-jobrunner:2021.6.0
- blackducksoftware/blackduck-cfssl:1.0.2
- blackducksoftware/blackduck-logstash:1.0.10
- blackducksoftware/blackduck-registration:2021.6.0
- blackducksoftware/blackduck-nginx:2.0.0
- blackducksoftware/blackduck-documentation:2021.6.0
- blackducksoftware/blackduck-upload-cache:1.0.17
- blackducksoftware/blackduck-redis:2021.6.0
- blackducksoftware/blackduck-bomengine:2021.6.0
- blackducksoftware/blackduck-matchengine:2021.6.0
- blackducksoftware/blackduck-webui:2021.6.0
- sigsynopsys/bdba-worker:2021.03
- blackducksoftware/rabbitmq:1.2.2

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.4.0が日本語にローカライズされました。

APIの機能強化

- ジョブサブシステムの変更:
 - GET /jobs/{jobID}は、特定のジョブの詳細をIDで取得する呼び出しです。この呼び出しは、404 Not Foundステータスコードを返します。
 - 次の呼び出しは、Black Duckバージョン2020.2.0以降では使用停止になり、404 Not Foundステータスコードを返し、Black Duckバージョン2021.6.0でも引き続き機能しません。
 - PUT /jobs/{jobID} これは、ジョブを再スケジュールする呼び出しです。
 - DELETE /jobs/{jobID} この呼び出しは、ジョブを終了します。
- この機能は、将来のリリースで利用可能になる新しいJob Rest APIの実装に変わります。
- 高速スキャンタイプを識別するために、ポリシービュー(/api/policy-rules/{policyRuleId})の式("developerScanExpression")に新しいブール値フィールドを追加しました。

2021.6.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (Hub-21613)。scan.cliバージョン2019.8.xで、使用しているJavaバージョンが原因でパフォーマンスが低下するという、意味のない警告メッセージが表示されていた問題が修正されました。

- ・ (Hub-25227、25521)。[スキャン]ページでスキャンのステータスがスキャン完了になり、誤解を招いていた問題が修正されました。
- ・ (Hub-26108)。Black DuckにAlertを展開する場合に、顧客証明書の使用時にnginxアラート設定ファイルを手動で操作しなければならなかった問題が修正されました。
- ・ (Hub-26924)。SAML SSOユーザーがログインに失敗したときに、ユーザーフレンドリーなエラーメッセージが表示されるように修正されました。
- ・ (Hub-27209)。VersionBomComputationJobが次のエラーで失敗していた問題が修正されました: "Error in job execution: could not extract ResultSet; SQL [n/a]; constraint [cvss2_severity]."
- ・ (Hub-27681)。カスタムセキュリティコンテキストを使用してKubernetesに展開するときに、ルートユーザーがBOM Engineを起動する必要があった問題が修正されました。
- ・ (Hub-27894)。新しいBlack Duck検索でリセットが0に設定されるように修正されました。
- ・ (Hub-28171)。1件のプロジェクトで著作権検索が失敗していた問題が修正されました。
- ・ (Hub-28305)。ログに次のエラーが表示されていた問題が修正されました: Failed class com.blackducksoftware.job.integration.domain.impl.JobMaintenanceJob
- ・ (Hub-28347)。スニペットの調整が重複キーSnippetAdjustmentエラーになっていた問題が修正されました。
- ・ (Hub-28351)。構成表ライセンスの変更を保存する際のパフォーマンスの問題が修正されました。
- ・ (Hub-28469)。Docker 20.10.xでカスタム証明書を設定できない可能性があった問題が修正されました。
- ・ (Hub-28726)。プロジェクトのクローンを作成した後に、プロジェクトのクローンを作成したユーザーの名前がコンポーネントレビュー担当者の名前としてBlack Duckに表示されていた問題が修正されました。
- ・ (Hub-28909)。ユーザー アカウントがロックアウトされた後、Black Duck UIに誤ったエラー メッセージが表示されていた問題が修正されました。
- ・ (Hub-29071)。スニペットを一括編集する際のパフォーマンスの問題が修正されました。
- ・ (Hub-29168)。プロジェクトバージョンにマッピングされたスキャンに一致するものがない場合に、プロジェクトレベルのファイル調整がそのプロジェクトバージョンに適用されなかった問題が修正されました。

Black Duck 2021.4.x

バージョン2021.4.1の新機能および変更された機能

Black Duck バージョン2021.4.1はメンテナンスリリースであり、新機能や変更された機能はありません。

2021.4.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (Hub-28347)。スニペットの一括調整が次のエラーで失敗していた問題が修正されました: "Adjustment Failed: The server encountered an error, please check your connection and try again."
- ・ (Hub-28807)。Artifactoryプラグインに次のエラーが表示されていた問題が修正されました: "Too many parameters error on /api/projects/<projectID>/versions/<projectVersionID>/components/<componentID>/versions/<componentVersionID>?offset=0&limit=100."
- ・ (Hub-29002)。[スニペット確認]ウィンドウで無視を解除されたスニペットをフィルタリングすると、システム全体のスニペットが表示されていた問題が修正されました。
- ・ (Hub-29448)。LDAPユーザー認証に失敗し、「IncorrectResultSizeDataAccessException」エラーが発生していた問題が修正されました。

バージョン2021.4.0の発表

新しいコンテナとシステム要件の変更

2021.6.0リリースでは、次のようになります。


- ・ 新しいコンテナblackduck-webuiが追加され、Black Duckのパフォーマンスの向上、キャッシュ機能の向上、将来の拡張性が実現されます。
- ・ 高速スキャン機能は、すべてのBlack Duckのお客様が使用できます。この機能を使用するには、現状ではblackduck-kbと呼ばれる新しいコンテナが必要です。このコンテナは、Black Duck KnowledgeBaseへの接続を管理し、KnowledgeBaseの結果を短い間隔でキャッシュします。

以下は、すべてのコンテナの単一インスタンスの実行に必要な最小ハードウェアです。メモリ要件は、サポートする同時高速スキャンの数によって異なることに、注意してください。

- ・ 7 CPU
- ・ Redisの最小構成の場合は28.5 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は31.5 GB RAM。これにより、最大100の同時高速スキャンがサポートされます。
Redisの最小構成の場合は30 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は33 GB RAM。これにより、150以上の高速スキャンがサポートされますが、サポートされる高速スキャンの最大数は現在判定中です。
- ・ データベースおよびその他のBlack Duckコンテナ用に250 GBの空きディスク容量
- ・ データベースバックアップに適した容量

以下は、Black Duck – Binary AnalysisでBlack Duckを実行するために必要な最小ハードウェアです。

- ・ 8 CPU
- ・ Redisの最小構成の場合は32.5 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は35.5 GB RAM。これにより、最大100の同時高速スキャンがサポートされます。
Redisの最小構成の場合は34 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は37 GB RAM。これにより、150以上の高速スキャンがサポートされますが、サポートされる高速スキャンの最大数は現在判定中です。
- ・ データベースおよびその他のBlack Duckコンテナ用に350 GBの空きディスク容量
- ・ データベースバックアップに適した容量

 注：binaryscannerコンテナを1個追加することにより、1 CPU、2 GB RAM、100 GBの空きディスク容量の追加が必要になります。

マップされていないコードの場所の保存期間

Black Duck 2021.6.0リリースでは、マップされていないコードの場所のデフォルトの保存期間が365日間から30日間に変更されます。

廃止されたAPI

次のエンドポイントは廃止され、今後のリリースでは削除される予定です。

`GET /api/scan/{scanId}/bom-entries`

次のエンドポイントは2021年4月30日をもって廃止されます。

`GET /api/components/{componentId}/versions/{componentVersionId}/origins/{originId}/direct-dependencies`

2021.6.0リリースでの新しいジョブ実装

Black Duckバージョン2021.6.0では、ジョブ サブシステムが新しい実装に変わっているため、以下のジョブのRest API呼び出しは機能しません。

- GET /jobs/{jobID}

この呼び出しは、特定のジョブの詳細をIDで取得します。Black Duck 2021.6.0リリースでは、この呼び出しは404 Not Foundステータス コードを返します。

次の呼び出しは、Black Duckバージョン2020.2.0以降では使用停止になり、404 Not Foundステータス コードを返し、Black Duckバージョン2021.6.0でも引き続き機能しません。

- PUT /jobs/{jobID}

これは、ジョブを再スケジュールする呼び出しです。

- DELETE /jobs/{jobID}

この呼び出しは、ジョブを終了します。

この機能は、将来のリリースで利用可能になる新しいJob Rest APIの実装に変わります。

日本語


UI、オンラインヘルプ、およびリリースノートのバージョン2021.2.0が日本語にローカライズされました。

バージョン2021.4.0の新機能および変更された機能

高速スキャン — お客様の使用が制限された機能

Black Duckの高速スキャンは、開発者が、プロジェクトに含まれているオープンソースコンポーネントのバージョンが、オープンソースの使用に関する企業ポリシーに違反しているかどうかを迅速に判断する方法を提供します。Black Duck Detectを使用すると、高速スキャンがパッケージマネージャのスキャンのみを使用し、Black Duckサーバーデータベースとやり取りしないので、迅速に結果が返されます。クイックフィードバックが必要な場合や、Black Duckでデータを保持する必要がない場合は、高速スキャンを使用します。

高速スキャンを使用すると、Black Duckの追加のインスタンスを展開しなくても、何千ものスキャンを実行できます。プロジェクトバージョンなしで、またはBlack Duckのユーザーインターフェイスにアクセスせずに使用できる、実用的な結果（ビルドの失敗など）を提供します。

 注：高速スキャンは、2021.4.0リリースの限定的なカスタマーアクセス機能です。高速スキャンを使用するには、Black Duckのアカウント管理チームにお問い合わせください。

重複している構成表の検出

Black Duck では重複している構成表の検出が追加されました。これは、新しいパッケージマネージャスキャンが既存の構成表を重複させるかどうかを判断し、重複させる場合はスキャンの処理を停止し、完了として指定します。冗長な（同一の）データを生成する高周波スキャンの場合、Black Duckの重複構成表検出により、パフォーマンスが大幅に向上します。

Black Duck 2021.4.0では、Black Duck Detectによって検出された一連の依存関係が前のスキャンのセットと同一の場合にのみ、この機能がパッケージ マネージャ（依存関係）スキャンに影響を与えます。この機能は今後のリリースで拡張される予定です。

プロジェクトマネージャの役割を構成する機能

Black Duck では、システム管理者が、プロジェクトマネージャの役割がポリシー違反を管理できるかどうか（ポリシー違反を上書きするか、上書きを削除するか）、またはプロジェクトのセキュリティ脆弱性を修正できるかどうかを定義できるようになりました。

デフォルトでは、プロジェクトマネージャの役割を持つユーザーは、ポリシー違反を管理し、セキュリティの脆弱性を修正できます。バージョン2021.4.0にアップグレードしたユーザーでは、プロジェクトマネージャの役割に変更はありません。

複数ライセンス編集の機能強化

KnowledgeBaseまたはカスタム コンポーネントのライセンスを編集するときに、Black Duckでは、ルート レベルまたは元のライセンスと同じレベルでコンポーネントの新しい複数ライセンス シナリオを簡単に作成したり、既存の複数ライセンス シナリオを編集したりできるようになりました。

ディープライセンスデータの機能拡張

Black Duck では、ファイル レベルのディープ ライセンスを追加したり、手動で追加したライセンスを削除したりできるようになりました。

レポートの機能強化

- ・ コンポーネントプロジェクトバージョンレポート (component_date_time.csv) では、次の機能が強化されています。
 - ・ 新しい列[コンポーネント取得元ID]がレポートの最後に追加されました。この列には、以前はAPIを使用してのみ取得できたコンポーネントの取得元ID値が表示されます。
 - ・ コメント列に一覧表示されている各コメントにユーザー名、日付、および時刻が追加されました。
- ・ アップグレードガイダンスプロジェクトバージョンレポート (project_version_upgrade_guidance_date_time.csv) の最後に、新しい列[ナレッジベースのタイムアウト]が追加されました。コンポーネントのバージョン/取得元のアップグレード ガイダンス データの取得中にBlack Duck KnowledgeBaseでタイムアウト エラーが発生したかどうかを示します。

ポリシー管理の機能強化

- ・ ポリシールールで使用可能なプロジェクトおよびコンポーネントの条件を、容易に見つけて選択できるようにするために、条件がカテゴリに再編成されました。また、プロジェクトとコンポーネントのカスタムフィールドは、カスタムフィールドのタイプによって分離されています。
- ・ 新しいライセンス条件である、宣言済みライセンスまたはディープライセンスの[ライセンスの有効期限の比較]では、ライセンスの有効期限をプロジェクトバージョンのリリース日と比較できます。

脆弱性の影響の機能強化

ポリシールールの新しい脆弱性条件[ソースから到達可能]が利用可能になり、到達可能と識別された脆弱性のポリシールールを作成できるようになりました。この条件を使用して、優先度が異なる(より高い)脆弱性に優先順位を付けます。

LDAPまたはSAMLグループの同期化の変更

認証エラーを減らすために、Black DuckはLDAPまたはSAMLグループの同期化を変更しました。現在は、LDAPまたはSAMLをBlack Duck用に設定するときにグループ同期を有効にした場合、LDAPまたはSAMLサーバー上のグループ名とBlack Duckサーバーが同一である必要があります。Black Duckでグループの名前を変更する場合は、LDAPまたはSAMLサーバー上のグループの名前も変更して、新しい名前に一致させる必要があります(その逆も同様です)。名前が同一でない場合、グループが同期されなくなる可能性があり、そのグループのユーザーの権限が失われます。

コンテナの拡張

Binaryscannerコンテナにヘルスチェックが追加されました。

[ソース]タブの機能強化

新しいフィルタ[コードビュー使用可能]がプロジェクトバージョンの[ソース]タブに追加されました。

コンポーネントおよびプロジェクト検索の機能強化

コンポーネントおよびプロジェクト検索の[検索]ページに、検索結果をソートする機能が追加されました。

保存済み検索の機能強化

ソートされた検索結果は、保存済み検索でサポートされており、ダッシュボードページで関心がある順序で結果を表示できます。

[プロジェクト名]ページのパフォーマンスの向上

パフォーマンスを向上させるには、ポリシー違反アイコン(🚫)または上書きアイコン(🔄)を選択して、[プロジェクト名]ページの[概要]タブにポリシー違反情報を表示する必要があります。

クローンの作成の機能強化

プロジェクトバージョンのクローンの作成に、次の機能強化が行われました。

- ・ デフォルトのクローンの作成オプションが変更されました。これで、プロジェクトの作成時にすべてのクローンの作成オプションが有効になります。
- ・ 新しいオプション[バージョン設定]が追加され、次の値のクローンが作成されます。
 - ・ ライセンス
 - ・ 注記
 - ・ ニックネーム
 - ・ リリース日
 - ・ フェーズ
 - ・ 配布
- ・ [プロジェクト名]ページから[クローン作成]選択すると、新しい[クローンバージョン]ダイアログボックスが表示されます。[バージョン設定]のクローン作成オプションが有効になっている場合は、新しいバージョン名のみがダイアログボックスに表示されます。
- ・ 混乱を避けるため、[クローンを作成するバージョン]フィールドは[新規バージョンを作成]ダイアログボックスから削除されました。

ライセンス競合の機能強化

[ライセンス競合]または[コンポーネント]タブを使用してコンポーネントまたはプロジェクトバージョンのライセンスの使用方法を変更するなど、構成表を手動で編集すると、ライセンス競合が再計算されます。

[システム情報]ページの機能強化

[システム情報]ページの使用カテゴリが拡張されました。

- ・ [使用方法:プロジェクト]セクションで、[プロジェクト別スキャン]セクションに[プロジェクト別上位10スキャン]が表示されるようになりました。
- ・ [使用方法:高速スキャン完了]セクションで、[ユーザー別高速スキャン]に[ユーザー別上位10の高速スキャン]が表示されるようになりました。

- ・ [使用方法: スキャン完了]セクションはテーブルに再フォーマットされ、重複している構成表の検出のための[同一パッケージマネージャ]行が含まれています。次の2つの新しいテーブルも追加されました。[コードの場所概要情報]と[重複構成表情報]です。

これらのページには、6か月のデータ、またはシステムにデータがある月数のいずれか小さい方が表示されます。

新しいジョブCollectScanStatsJobは、[システム情報]ページの[使用方法: スキャン完了]セクションに表示されるスキャン統計情報を収集します。

インストールガイドの削除

「Kubernetesを使用したBlack Duckのインストール」および「OpenShiftを使用したBlack Duckのインストール」ガイドがドキュメントセットから削除されました。これらのドキュメントには、最新のドキュメントへのリンクのみが含まれていました。これらのリンクは、各PDFのBlack Duckドキュメント ページおよびオンライン ヘルプのホームページに追加されています。

[プロジェクト名]ページの機能強化

[プロジェクト名]ページが再編成されて強化され、各プロジェクトバージョンの最後のスキャン日が含まれるようになりました。

[ダッシュボード]ページの機能強化

[ダッシュボード]ページのポリシー違反円グラフの「なし」のポリシー違反値は、以前は100% (違反なし) または0% (いくつかの違反) のどちらかを返していましたが、違反の実際の割合を反映するようになりました。

サポートされるブラウザのバージョン

- ・ Safariバージョン14.0.3 (15610.4.3.1.7、15610)
- ・ Chromeバージョン90.0.4430.72 (公式ビルド) (x86_64)
- ・ Firefoxバージョン88.0 (64ビット)
- ・ Microsoft Edgeバージョン90.0.818.41 (公式ビルド) (64ビット)

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:1.0.16
- ・ blackducksoftware/blackduck-authentication:2021.4.0
- ・ blackducksoftware/blackduck-webapp:2021.4.0
- ・ blackducksoftware/blackduck-scan:2021.4.0
- ・ blackducksoftware/blackduck-jobrunner:2021.4.0
- ・ blackducksoftware/blackduck-cfssl:1.0.1
- ・ blackducksoftware/blackduck-logstash:1.0.9
- ・ blackducksoftware/blackduck-registration:2021.4.0
- ・ blackducksoftware/blackduck-nginx:1.0.31
- ・ blackducksoftware/blackduck-documentation:2021.4.0
- ・ blackducksoftware/blackduck-upload-cache:1.0.16
- ・ blackducksoftware/blackduck-redis:2021.4.0
- ・ blackducksoftware/blackduck-bomengine:2021.4.0

- ・ sigsynopsys/bdba-worker:2021.03
- ・ blackducksoftware/rabbitmq:1.2.2

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2021.2.0が日本語にローカライズされました。

APIの機能強化


- ・ APIドキュメントでPostmanコレクションを生成する機能を、/api-doc/postman-collection-public.jsonから追加しました。ユーザーは、PostmanコレクションとしてPostmanにpostman-collection-public.jsonファイルをインポートできます。
- ・ /api-doc/openapi3-public.jsonを介してお客様向けエンドポイントのOpenAPI Specification (OAS)を生成する機能を追加しました。
- ・ /api/projects?filter=ownerを使用してプロジェクト所有者別にプロジェクトをフィルタリングする機能を追加しました。この機能はユーザーのURLを取得してユーザーが所有するプロジェクト(例: /api/projects?filter=owner:https://<bd_server>/api/users/)を検索します。
- ・ ライセンス所有権情報を新しい所有権フィールドとして/projects/{projectId}/versions/{projectVersionId}/componentsエンドポイントに追加しました。
- ・ 次のアプリケーション設定を読み取り、変更するためのAPIが追加されました。
 - ・ 分析設定の読み取り
GET /api/settings/analysis
 - ・ 解析設定の更新
PUT /api/settings/analysis
 - ・ ブランディング設定の読み取り
GET /api/settings/branding
 - ・ ブランディング設定の更新
PUT /api/settings/branding
 - ・ ライセンスレビュー設定の読み取り
GET /api/settings/license-review
 - ・ ライセンスレビュー設定の更新
PUT /api/settings/license-review
 - ・ 役割設定の読み取り
GET /api/settings/role
 - ・ 役割設定の更新
PUT /api/settings/role
- ・ 特定の日付または特定のコンポーネントに基づいてナレッジベースからコンポーネントの移行データを取得するための/api/component-migrationsおよび/api/component-migrations/{componentOrVersionId}エンドポイントが追加されました。
- ・ /license-dashboardAPIを公開し、ユーザーが使用中のライセンスを表示できるようにしました。
- ・ 脆弱性が100を超える参照を持っている場合に、api/vulnerabilities/{vulnerabilityId}エンドポイントがヘッダーオーバーフローエラーを返す問題を解決しました。エンドポイントは警告を表示し、応答ヘッダーで25以上のリンクヘッダーが返されたときに、応答本文にメタリンクを含めます。

- ・ [トリガータイプ]フィルタは[ユーザー]タイプにのみ使用されるため、このフィルタをアクティビティ/ジャーナルエンドポイントから削除しました。

2021.4.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (Hub-24015, 26281)。Black Duckユーザーインターフェイスに表示されていた断続的なアクセス権限拒否エラーが修正されました。
- ・ (HUB-25116)。UCS-2でエンコードされたファイルの[スニペットビュー]ダイアログボックスに赤いドットが表示され、テキストが読み取れなかった問題が修正されました。
- ・ (HUB-25549)。codeLocationNameに日本語の文字が含まれている場合に、作成されたコードの場所がプロジェクトバージョンにマップされなかった/api/uploadsの問題が修正されました。
- ・ (HUB-25550)。プロジェクトバージョンのアクティビティ/ジャーナルに構成表更新日時を追加しました。
- ・ (HUB-25605, 27618)。/api/tokens/authenticateを使用してAPIトークンで認証を行う場合の問題が修正されました。この問題では、トークンの期限が切れた後に、HTTPクライアントがSAMLプロバイダページにリダイレクトされるか、PDFレポートの生成中にエラーが発生していました。
- ・ (Hub-25993)。重複したレコードが原因で、Job Runnerログに次のエラーメッセージが表示されていた問題が修正されました。「A conflicting object already exists」
- ・ (Hub-26481)。新しい修正ステータスを保存した後に、ページが完全に更新されていた問題が修正されました。
- ・ (HUB-26588)。android-studio-ide-201.7199119-windows.exeでバイナリスキャンを実行できなかった問題が修正されました。
- ・ (Hub-26695)。一日の特定の時間帯にスキャンにかなり時間がかかっていた問題が修正されました。
- ・ (Hub-26897)。[コンポーネント名]ページに一覧表示されていない無効なバージョンについて、404 Not Foundエラーコードが表示されるように修正しました。
- ・ (Hub-26911)。代替スニペットマッチを選択したときに、コンポーネントが暗号化されていると誤って識別されていた問題が修正されました。
- ・ (Hub-27159)。「過去1年間のコントリビュータ」、「過去1年間のコミット」、または「新しいバージョン数」コンポーネント条件を使用するポリシールールの問題が修正されました。これらの条件は、値が0の場合に違反をトリガーするように定義されていますが、値が0より大きい場合、またはコンポーネントにコミット履歴がない場合にポリシー違反がトリガーされました。

 注：この修正により、新しいスキャンまたは再スキャンによって、以前にトリガーされたいくつかのポリシー違反が削除されることがあります。

- ・ (Hub-27167)。グローバルプロジェクトビューアの役割を持つ非アクティブなグループに割り当てられたアクティブなユーザーが、ダッシュボードですべてのプロジェクトを表示できていた問題が修正されました。
- ・ (Hub-27175)。[コンポーネント名]ページの[使用数]の値が、コンポーネントのバージョンではなく、コンポーネントの取得元の数に基づいていたために不正確だった問題が修正されました。
- ・ (Hub-27282)。構成表のポリシー違反ポップアップが開いたままになっていることがあり、ページを更新しない限り閉じられなかった問題が修正されました。
- ・ (Hub-27284, 27660)。推移的な依存関係のマッチタイプを持つ一部の動的にリンクされたコンポーネントで、プロジェクトバージョン構成表の[ソース]列にマッチ情報が欠落していた問題が修正されました。
- ・ (Hub-27287)。[プロジェクト名]ページの[概要]タブに表示されるリスク数が、コンポーネント取得元ではなく、コンポーネントのバージョン値を使用するように([構成表]ページと同じように)、問題を修正しました。
- ・ (Hub-27293)。「レビュー済み」とマークされたコンポーネントが、プロジェクトの再スキャン時に「未レビュー」とマークされていた問題が修正されました。

- ・ (Hub-27306)。通知レポートでコンポーネントが大文字と小文字を区別する順序で一覧表示されていた問題が修正されました。
- ・ (Hub-27308)。コンポーネントバージョンのライセンスが変更された後、Black Duck KB [コンポーネント名] ページに脆弱性の数が正しく表示されていなかった問題が修正されました。
- ・ (Hub-27326)。プロジェクトの[設定]タブを使用してアプリケーションIDを削除しても、実際にはアプリケーションIDが削除されていなかった問題が修正されました。
- ・ (Hub-27613)。[ソース]タブでバイナリのソースファイルに移動できなかった問題が修正されました。
- ・ (Hub-27961)。[ダッシュボード]ページのグラフの凡例を修正し、クリック可能な状態で表示されないようにしました。
- ・ (Hub-27982)。バイナリスキャンでMSIアーカイブの最初と最後のファイルのみが識別されていた問題が修正されました。
- ・ (Hub-27985)。Black Duckが構成表を作成しているときに表示されるメッセージが、構成表ページを下にスクロールすると表示されなくなっていた問題が修正されました。
- ・ (Hub-28094)。/api/usergroupsエンドポイントが検索語で「_」または「%」を正しく使用していなかった問題が修正されました。
- ・ (Hub-28165)。構成表ページでライセンスを編集する際に[キャンセル]/[閉じる]を選択しても変更が適用されていた問題が修正されました。
- ・ (Hub-28208)。[登録]ページに表示されるコードベースサイズが正しくなかった問題が修正されました。
- ・ (Hub-28226)。1つまたは複数のポリシーに違反しているコンポーネントが、そのコンポーネントが配置されたコードの場所がマップされていないか削除された場合に、「ポリシークリア済み」通知を生成するように修正されました。
- ・ (Hub-28259)。SQLクエリ解析の「未レビュー/無視を解除」に関する問題が修正されました。
- ・ (Hub-28292)。HELM Tシャツのサイズ設定.ymlファイルが構成表エンジンコンテナをスケールしなかった問題が修正されました。
- ・ (Hub-28370)。構成表の比較ビューを使用しているときに重大な脆弱性が表示されていなかった問題が修正されました。
- ・ (Hub-28375)。CVEまたはBDBAレコードの[影響を受けるプロジェクト]タブに無視されたコンポーネントの脆弱性が表示されないように、問題を修正しました。
- ・ (Hub-28383)。[プロジェクト名]ページがフィルタにかけられ、結果としてページに1つのバージョンしか表示されない場合に、バージョンを削除できなかった問題を修正しました。
- ・ (Hub-28416)。ライセンスのグループのANDまたはOR演算子を変更できなかった問題が修正されました。
- ・ (Hub-28458)。SnippetScanAutoBomジョブで「Error in job execution: Duplicate key」エラーメッセージが表示される問題が修正されました。
- ・ (Hub-28562)。スキャンが事後処理を完了できず、次のエラーメッセージが表示されていたバイナリスキャンの問題が修正されました。「Path is not a parent of null。」
- ・ (Hub-28580)。[マイアクセストークン]ページにアクセスしようとすると、エラー「アプリケーションに不明なエラーが発生しました」が発生していた問題が修正されました。
- ・ (Hub-28639)。プロジェクト名に英語と中国語の両方の文字が含まれている場合、ダウンロードしたレポートファイルのサフィックスに.zipの代わりに.json拡張子が付いていた問題が修正されました。
- ・ (Hub-28681)。マッチタイプが直接または推移的な依存関係である場合に、[ソース]タブに使用状況が表示されるように、問題を修正しました。
- ・ (Hub-28765)。[構成表]ページに確認済みと無視済みの両方のスニペットが表示されていた問題が修正されました。

- ・ (Hub-28773)。hub-webserver.envファイルのTLS_PROTOCOLSオプションからTLSv1.1が削除されるように、問題を修正しました。

Black Duck 2021.2.x

バージョン2021.2.1の新機能および変更された機能

Black Duck バージョン2021.2.1はメンテナンスリリースであり、新機能や変更された機能はありません。

2021.2.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (Hub-23928)。確認済みスニペットマッチが再スキャン後に変更されていた問題が修正されました。
- ・ (Hub-26898)。スキャンが完了したように見えても、Black Duckからbom_complete通知を取得できなかったためにBlack Duck Detectがタイムアウトしていた問題が修正されました。
- ・ (Hub-27688)。マッチしたファイルのAPI呼び出しで、推移的な依存関係と直接の依存関係のマッチに関する情報が返されなかった問題が修正されました。
- ・ (Hub-28410)。KubernetesでRabbitMQコンテナを起動できなかった問題が修正されました。この問題は永続的ボリュームを導入することで解決されました。
- ・ (Hub-28208、28386)。[製品登録]ページに誤ったコードベースサイズが表示されていた問題が修正されました。
- ・ (Hub-28278)。RabbitMQコンテナの永続ボリュームが見つからないために構成表エンジンに過剰なログが記録され、スキャンが失敗していた問題が修正されました。
- ・ (Hub-28292)。構成表エンジンコンテナのスケーリングに関する問題が修正されました。

バージョン2021.2.0の発表

Azureをご利用のお客様へのお知らせ

Black Duck バージョン2021.2.0は、Azure Kubernetes Services (AKS) で展開し、Azure Database for PostgreSQLを外部データベースとして使用するお客様に影響を与える既知の問題とともにリリースされています。これは、Azure プラットフォーム上のBlack Duckのお客様に推奨される標準構成であることに注意してください。現時点では、外部データベースを備えたAzureプラットフォームで実行しているお客様が2021.2.0にアップグレードすることはお勧めしません。これを行うと、システムが動作不能のままになり、インストールを前の状態に戻すように強制されます。

この問題は今後のBlack Duckリリースで解決される予定であり、リリースの詳細が判明した時点で発表されます。

AKS上で実行しており、内部PostgreSQLデータベースを使用する場合は、問題はなく、システムは期待どおりに動作します。ただし、これは、AKSプラットフォームでの変則的なインストールです。

ご不明な点やご質問がある場合は、Black Duckサポートにお問い合わせください。

外部データベース用のPostgreSQLバージョン9.6のサポート廃止

Black Duck は、Black Duck 2021.6.0リリース以降で、外部データベース用のPostgreSQLバージョン9.6のサポートを廃止する予定です。

Black Duck 2021.6.0リリース以降では、Black Duckは、外部データベース用にPostgreSQLバージョン11.xのみをサポートします。

Internet Explorer 11はサポートされなくなりました

Black Duck はInternet Explorer 11のサポートを終了しました。

廃止されたページ

[スキャン] > [コンポーネント] ページは、2021.2.0リリースで廃止され、今後のリリースでは削除される予定です。

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2020.12.0が日本語にローカライズされました。

バージョン2021.2.0の新機能および変更された機能

新しいカスタム脆弱性ダッシュボード

2021.2.0では、セキュリティダッシュボードが、保存済み脆弱性検索を使用できるカスタム脆弱性ダッシュボードに切り替わり、重要な脆弱性を簡単に表示できるようになりました。Black Duck では、さまざまな属性を使用してプロジェクトおよび/またはBlack Duck KnowledgeBase内で使用される脆弱性を検索し、検索を保存してから、この[ダッシュボード] ページを使用して保存済み検索からダッシュボードを表示できるようになりました。

脆弱性ごとに、カスタム脆弱性ダッシュボードに次の情報が表示されます。

- ・ BDSAまたはNVDの脆弱性ID。脆弱性IDを選択すると、追加のスコア値など、脆弱性に関する詳細情報が表示されます。
- ・ この脆弱性の影響を受けるプロジェクトのバージョンの数と、この脆弱性の影響を受けるプロジェクトのバージョンが一覧表示された脆弱性の[影響を受けるプロジェクト]タブを表示するリンク。
- ・ 全体的なリスクスコア。
- ・ ソリューション、回避策、または攻撃が利用可能かどうか。
- ・ 脆弱性が最初に検出、公開、および最終変更された日付。
- ・ このセキュリティ脆弱性の共通脆弱性タイプ一覧(CWE)番号。

脆弱性検索の機能強化

脆弱性の検索は、脆弱性の検索に使用できる属性と、検索結果に表示される情報によって強化されています。プロジェクトの脆弱性を検索するか、Black Duck KnowledgeBaseの脆弱性を検索するかどうかを選択できます。

脆弱性を検索する場合は、次の属性を使用できます。

- ・ 影響を与えるプロジェクト
- ・ デフォルトの修正
- ・ 到達可能
- ・ 悪用
- ・ 最初の検出
- ・ 修正ステータス
- ・ 解決方法
- ・ ベーススコア
- ・ 攻撃される可能性のスコア
- ・ 影響スコア

- ・ 総合スコア
- ・ 公開された年
- ・ 重大度
- ・ ソース(BDSAまたはNVD)
- ・ 一時スコア
- ・ 回避策

これらの脆弱性は、前述のように、検索結果を保存して[ダッシュボード]ページに表示できるようになりました。

プロジェクトのライセンス競合を管理する機能

ライセンス違反のリスクを軽減するため、構成表内のコンポーネントに、プロジェクトの宣言されたライセンスに対して齟齬がある条項を含むライセンスがある場合を理解する必要があります。Black Duck では、これらのライセンス条項の競合を特定し、それを[法]タブにある新しい[ライセンス競合]に表示するようになりました。

コンポーネントのライセンスがプロジェクトバージョンのライセンスと競合する場合にトリガーされるポリシールールを設定することもできます。

Black Duckは、ライセンスのリスクが高いコンポーネントバージョンに対するライセンス競合のみを判断することに注意してください。Black Duckライセンスリスクモデルにおける「高リスク」とは、このビジネスシナリオ(配布タイプとコンポーネントの使用法の組み合わせ)の下で、このファミリのライセンスが競合する傾向があることを意味します。中程度または低リスクとは、ビジネスシナリオが変更された場合(または誤って定義された場合)、またはライセンス以外の競合要因が原因でリスクが発生する可能性があることを意味します。

依存関係

Black Duck Detectスキャンで直接的または推移的な依存関係が検出された場合、Black Duckは、プロジェクトバージョンの[セキュリティ]タブで、依存関係の各タイプの一致数を一覧表示するようになりました。

推移的な依存関係の場合、依存関係ツリーには、この依存関係をもたらしたコンポーネント、重大度レベル別の脆弱性、およびその依存関係パスでコンポーネントが導入された回数のマッチ数が表示されます。

レポートデータベースの機能強化

無視されたコンポーネントの新しいテーブル(component_ignored)がレポートデータベースに追加されました。次のカラムがあります。

- ・ id。ID
- ・ project_version_id。プロジェクトバージョンID。
- ・ component_id。コンポーネントID。
- ・ component_version_id。コンポーネントバージョンID。
- ・ component_name。コンポーネント名。
- ・ component_version_name。コンポーネントバージョン名。
- ・ version_origin_id。バージョン取得元ID。
- ・ origin_id。取得元ID。
- ・ origin_name。取得元名。
- ・ ignored。コンポーネントが無視されるかどうかを示すブール値。
- ・ policy_approval_status。ポリシーの承認ステータス。
- ・ review_status。コンポーネントのレビューステータス。

- ・ reviewed_by。コンポーネントをレビューしたユーザー。
- ・ reviewed_on。コンポーネントがレビューされた日時。
- ・ security_critical_count。重要なセキュリティ脆弱性の数。
- ・ security_high_count。高セキュリティ脆弱性の数。
- ・ security_medium_count。中程度のセキュリティ脆弱性の数。
- ・ security_low_count。低セキュリティ脆弱性の数。
- ・ security_ok_count。セキュリティの脆弱性が存在しない数。
- ・ license_high_count。高ライセンスリスクの数。
- ・ license_medium_count。中ライセンスリスクの数。
- ・ license_low_count。低ライセンスリスクの数。
- ・ license_ok_count。ライセンスリスクなしの数。
- ・ operational_high_count。高い運用リスクの数。
- ・ operational_medium_count。中程度の運用リスクの数。
- ・ operational_low_count。低い運用リスクの数。
- ・ operational_ok_count。運用リスクなしの数。

ユーザー情報の新しいテーブル (user) がレポートデータベースに追加されました。次のカラムがあります。

- ・ id。ID。
- ・ first_name。ユーザーの名。
- ・ last_name。ユーザーの姓。
- ・ username。Black Duckのユーザーのユーザー名。
- ・ email。ユーザーの電子メールアドレス。
- ・ active。このユーザーがアクティブかどうかを示すブール値。
- ・ last_login。ユーザーがBlack Duckに最後にログインした時刻。

ライセンス編集の機能強化

構成表でライセンスを編集する際に、次の機能強化が行われました。

- ・ コンポーネントのライセンスを編集するときに、Black Duckでは、ルート レベルまたは元のライセンスと同じレベルで構成表内のコンポーネントの新しい複数ライセンス シナリオを簡単に作成したり、既存の複数ライセンス シナリオを編集したりできるようになりました。
- ・ コンポーネントに別のライセンスを選択した場合は、Black Duck KnowledgeBaseで定義されたとおりに、ライセンスを元のライセンスに戻すことができます。
- ・ [＜コンポーネント名 バージョン＞コンポーネントライセンス]ダイアログボックスの新しいオプションにより、編集モードがあることを容易に識別できます。

レポートの機能強化

source_date_time.csvプロジェクトバージョンレポートの最後に、新しいカラム[アーカイブのコンテキストとパス]が追加されました。このカラムは、既存のパスとアーカイブコンテンツのカラムに表示される情報を連結して、各コンポーネントのフルパスを提供します。

通知ファイルレポート

通知ファイルレポートが改善され、著作権データに単一のコンポーネント取得元の重複情報が含まれなくなりました。

バイナリスキャンの機能拡張

バイナリスキャンでは、完全一致に加えて部分一致が返されるようになりました。


ディープライセンスデータの機能拡張

ファイル内のディープライセンスデータの証拠を確認するときに、Black Duckでは、ライセンステキストの一致をトリガーしたライセンステキストが強調表示されるようになりました。

BOM Engine

Black Duck UIの応答時間を改善するために、ライセンスの更新はBOM Engineによって実行されるようになりました。このプロセスは、構成表からアクセス可能な[構成表処理ステータス]ダイアログボックスで、[ライセンスの更新]または[ライセンス条項の履行の更新]イベントとして表示されます。

Black Duck チュートリアル

Black Duckのトレーニングを簡単に表示するには、[ヘルプ]メニューからBlack Duckのチュートリアル() (Black DuckのUIに表示)を選択してください。

パスワードの構成の変更

システム管理者のロールを持つユーザーは、ローカル Black Duck アカウントのパスワード要件を設定できるようになりました。スーパーユーザーの役割を持つユーザーは、パスワード要件を構成できなくなりました。

ポリシールールの機能強化

ポリシー管理では、ブール値、日付、ドロップダウン、複数選択、単一選択、およびテキストフィールドタイプのプロジェクトバージョンのカスタムフィールドに基づいて、ポリシールールを作成する機能が提供されるようになりました。




ホスティングロケーション: Black Duck Detect

Black Duck 外部接続が制限されているお客様は、Black Duck Detectの内部ホスティング ロケーションを定義できるようになりました。これらのユーザーは、この情報を使用して、Code Sightを利用して開発者ベース全体に展開し、オンデマンドのソフトウェアコンポジション解析(SCA)スキャンを実行できます。

保存済み検索ダッシュボードの機能強化

[ダッシュボード]ページに表示される保存済み検索ごとに、検索が最後に更新された日時がBlack Duckに一覧表示されるようになりました。ポップアップに保存された検索フィルタとリンクが表示されるので、[検索]ページを開いて、改訂された保存済み検索を編集および保存できます。

スニペットのトリアージの機能拡張

未確認スニペット()、確認済みスニペット()、無視されたスニペット()を区別しやすくするために、[ソース]タブにアイコンが追加されました。

サポートされるブラウザのバージョン

- ・ Safariバージョン14.0.3(15610.4.3.1.6, 15610)

- ・ Chromeバージョン88.0.4324.150(公式ビルド)(x86_64)
- ・ Firefoxバージョン85.0.2(64ビット)
- ・ Microsoft Edgeバージョン88.0.705.63(公式ビルド)(64ビット)

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:1.0.16
- ・ blackducksoftware/blackduck-authentication:2021.2.0
- ・ blackducksoftware/blackduck-webapp:2021.2.0
- ・ blackducksoftware/blackduck-scan:2021.2.0
- ・ blackducksoftware/blackduck-jobrunner:2021.2.0
- ・ blackducksoftware/blackduck-cfssl:1.0.1
- ・ blackducksoftware/blackduck-logstash:1.0.9
- ・ blackducksoftware/blackduck-registration:2021.2.0
- ・ blackducksoftware/blackduck-nginx:1.0.30
- ・ blackducksoftware/blackduck-documentation:2021.2.0
- ・ blackducksoftware/blackduck-upload-cache:1.0.15
- ・ blackducksoftware/blackduck-redis:2021.2.0
- ・ blackducksoftware/blackduck-bomengine:2021.2.0
- ・ sigsynopsys/bdba-worker:2020.12-1
- ・ blackducksoftware/rabbitmq:1.2.2

サポートされるDockerのバージョン

Black Duck のインストールでは、Dockerバージョン18.09.x、19.03.x、および20.10.x(CEまたはEE)がサポートされています。

Docker webapp-volume

Docker webapp-volumeは、オーケストレーションでは使用されなくなりました。必要に応じて、ユーザーはDocker webapp-volumeをバックアップおよびプルーニングできます。それ以外の場合は、アクションは必要ありません。

Ubuntuオペレーティングシステム

UbuntuのDocker環境にBlack Duckをインストールするための推奨オペレーティング システムは、バージョン18.04.xです。

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2020.12.0が日本語にローカライズされました。


APIの機能強化

- ・ APIドキュメントは、<https://<Black Duck server URL>/api-doc/public.html>でのみ入手できるようになりました。
- ・ 作成日でコードの場所(/api/codelocations)をフィルタリングする機能が追加されました。

- ・ 以前のバージョンで正しく動作していなかった、SAML Identity ProviderメタデータXMLファイル (api/sso/idp-metadataエンドポイント) のダウンロードに使用されるAPIが修正されました。
- ・ remediation-guidanceエンドポイント (GET /api/components/{componentId}/versions/{componentVersionId}/remediating) は、「410 GONE」応答を返さなくなりました。upgrade-guidanceエンドポイント (GET /api/components/{componentId}/versions/{componentVersionId}/upgrade-guidance) に切り替える必要があります。このエンドポイントは、削除されたremediation-guidanceエンドポイントと互換性がありません。
- ・ コンポーネントの依存関係パスを表示するために、レポートのdependency-pathsエンドポイントが追加されました。
/api/project/{projectId}/version/{projectVersionId}/origin/{originId}/dependency-paths
- ・ [システム設定] ページでBlack Duck Detect URIの読み取りを設定または更新するためにのみ使用されるBlack Duck Detect URIエンドポイントが追加されました。
/external-config/detect-uri

2021.2.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (Hub-22103)。ライセンスステータスを更新するときに、Black Duckサーバーが時間内に応答しなかった問題が修正されました。
- ・ (Hub-22623)。UIにロードするときに、概要ダッシュボードが企業顧客に対して頻繁にタイムアウトしていた問題が修正されました。
- ・ (Hub-24332)。同じコードの場所をスキャンすると通知が重複していた問題が修正されました。
- ・ (Hub-25374)。データベースazure_maintenanceの権限エラーが修正されました。
- ・ (Hub-25580)。構成表に表示されているコンポーネントが9ページ以降で正しくソートされていなかった問題が修正されました。
- ・ (Hub-25666)。エンドポイント/usergroups/<group #>/rolesのページネーションの問題が修正されました。
- ・ (Hub-26030)。アクションの実行後に、ダッシュボードのソートオプションがプロジェクト名で保持されなかった問題が修正されました。
- ・ (Hub-26324)。エラー「java.lang.IllegalStateException: Parent of [file:/C:/src/External/PackageManager/ProjectTemplates/com.unity.template.universal-10.1.0.tgz] does not exist」がスキャンのアップロード時に発生していた問題が修正されました。
- ・ (Hub-26343)。登録コンテナのヒープ領域が不足しているため、Black Duckを登録できなかった問題が修正されました。
- ・ (Hub-26493)。ユーザーがプロジェクトのメンバーとして自分自身を削除したときに表示されていた紛らわしいエラーメッセージが修正されました。
- ・ (Hub-26501)。[コンポーネントの編集] ダイアログボックスでcordova-plugin-inappbrowserコンポーネントを選択できなかった問題が修正されました。
- ・ (Hub-26536)。ウォッチするプロジェクトがページヘッダーにウォッチしないアイコン()を表示していた問題が修正されました。
- ・ (Hub-26540)。Black Duckを再起動しないとSAMLの初期構成が有効にならなかった問題が修正されました。
- ・ (Hub-26615)。プロジェクトAでプロジェクトマネージャの役割を持ち、プロジェクトBでプロジェクトマネージャとプロジェクトコードスキャナの役割を持つユーザーが、スキャンをプロジェクトAにアップロードできていた問題が修正されました。

- ・ (Hub-26616)。スニペットを無視しようとする、次のエラーメッセージで失敗する可能性があった問題が修正されました。「コンシューマ、プロデューサー、調整タイプ、開始行、終了行の変更がサポートされていないため、既存のスニペット調整を更新できません。」
- ・ (Hub-26712、26962)。スニペットマッチが確認された後、[ソース]タブのツリービューに表示されるスニペットアイコンがクリアされなかった問題を修正しました。
- ・ (Hub-26726)。ポリシールールを作成するときに、カスタムフィールドで「not in」オプションを使用できなかった問題が修正されました。
- ・ (Hub-26807)。構成表コンポーネントバージョンのカスタムフィールドを取得しようとしたときに、HTMLステータスコード404を受信していた問題が修正されました。
- ・ (Hub-26815)。SAML統合設定を保存するとページが再ロードされ、Identity Providerメタデータ設定が切り替わっていた問題が修正されました。
- ・ (Hub-26904)。[設定]タブのプロジェクトバージョンの[アクティビティ]セクションに表示されるマッチ数値が[スキャン名]ページと異なっていた問題を修正しました。
- ・ (Hub-26930)。コンポーネントの通知がトリガーされなかった問題が修正されました。
- ・ (Hub-27002)。クローン作成されたプロジェクトが作成されたときに誤った通知が送信されていた問題が修正されました。
- ・ (Hub-27049)。ユーザーにライセンスマネージャのロールが割り当てられていないと、プロジェクトバージョンレポートのライセンス条項カテゴリが、Black Duck UIに表示されなかった問題が修正されました。
- ・ (Hub-27208)。SAMLの構成時にBlack Duck Alertの読み込みに失敗していたblackduck-nginxの問題が修正されました。
- ・ (Hub-27227)。スニペットのマッチングが完了するまでに長時間を要していた問題が修正されました。
- ・ (Hub-27264)。コンポーネントを確認すると、その使用状況がデフォルト値にリセットされていた問題が修正されました。
- ・ (Hub-27681)。カスタムセキュリティコンテキストを使用してKubernetesに展開するときに、ルートユーザーがBOM Engineを起動する必要がある問題が修正されました。

Black Duck 2020.12.x

バージョン2020.12.0の発表

新しいコンテナとシステム要件の変更

新しいコンテナが2つ追加されています。2020.12.0リリース向けのBOM EngineおよびRabbitMQ（今後は必須コンテナ）です。


すべてのコンテナの単一インスタンスを実行するための最小システム要件は次のとおりです。

- ・ 6 CPU
- ・ Redisの最小構成の場合は26 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は29 GB RAM
- ・ データベースおよびその他のBlack Duckコンテナ用に250 GBの空きディスク容量
- ・ データベースバックアップに適した容量

Black Duck – Binary AnalysisでBlack Duckを実行するために必要な最小ハードウェアは次のとおりです。

- ・ 7 CPU

- ・ Redisの最小構成の場合は30 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は33 GB RAM
- ・ データベースおよびその他のBlack Duckコンテナ用に350 GBの空きディスク容量
- ・ データベースバックアップに適した容量

 注： binaryscannerコンテナを1個追加することにより、1 CPU、2 GB RAM、100 GBの空きディスク容量の追加が必要になります。

Internet Explorer 11のサポートの終了

Internet Explorer 11のサポートは廃止されます。Black Duckは、Black Duck 2021.2.0 リリース以降でのInternet Explorer 11のサポートを終了します。

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2020.10.0が日本語にローカライズされました。

バージョン2020.12.0の新機能および変更された機能

新しいコンテナとシステム要件の変更


新しいコンテナが2つ追加されています。2020.12.0リリース向けのBOM EngineおよびRabbitMQ (今後は必須コンテナ)です。

すべてのコンテナの単一インスタンスを実行するための最小システム要件は次のとおりです。

- ・ 6 CPU
- ・ Redisの最小構成の場合は26 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は29 GB RAM
- ・ データベースおよびその他のBlack Duckコンテナ用に250 GBの空きディスク容量
- ・ データベースバックアップに適した容量

Black Duck – Binary AnalysisでBlack Duckを実行するために必要な最小ハードウェアは次のとおりです。

- ・ 7 CPU
- ・ Redisの最小構成の場合は30 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は33 GB RAM
- ・ データベースおよびその他のBlack Duckコンテナ用に350 GBの空きディスク容量
- ・ データベースバックアップに適した容量

 注： binaryscannerコンテナを1個追加することにより、1 CPU、2 GB RAM、100 GBの空きディスク容量の追加が必要になります。

パスワードの構成

スーパーユーザーのロールを持つユーザーが、ローカル Black Duck アカウントのパスワード要件を設定できるようになりました。有効にすると、新しいパスワードがお客様の要件を満たしていることが、Black Duckにより確認されます。また、脆弱と見なされるパスワード(「password」、「blackduck」、ユーザーのユーザー名や電子メールアドレスなど)は拒否されます。

スーパーユーザーは次の操作を実行できます。

- ・ 最小パスワード長を定義します。
- ・ パスワードの最小文字種数を定義します。使用可能な文字種は、小文字、大文字、数字、特殊文字です。

- ・ 現在のユーザーがBlack Duckにログインするときにパスワード要件を適用するかどうかを選択します。デフォルトでは、パスワード要件は有効で、次のように設定されています。
- ・ 最小パスワード長は8文字です。
- ・ 必要な文字種は1つだけです。
- ・ Black Duckにログインしている現在のユーザーには、パスワード要件が適用されません。

ライセンスの機能強化

ライセンスリスクを適切に管理できるように、Black Duckでは、構成表のコンポーネントについてマルチライセンスシナリオを新規に作成したり既存のものを編集したりできるようになりました。

脆弱性の影響解析の機能強化

- ・ 新しいプロジェクトバージョンレポートvulnerability_matches_date_time.csvが追加されました。脆弱性によって到達される可能性のあるコンポーネントごとに、コンポーネント、脆弱性データ、および脆弱性の影響解析データが一覧表示されます。このレポートには、次のカラムがあります。
 - ・ コンポーネント名
 - ・ コンポーネントID
 - ・ 使用中
 - ・ コンポーネントバージョン名
 - ・ バージョンID
 - ・ チャンネルバージョン取得元
 - ・ 取得元ID
 - ・ 取得元名ID
 - ・ 脆弱性ID
 - ・ 脆弱性ソース
 - ・ CVSSバージョン
 - ・ セキュリティ上のリスク
 - ・ ベーススコア
 - ・ 総合スコア
 - ・ ソリューションが利用可能
 - ・ 回避策が利用可能
 - ・ 攻撃が利用可能
 - ・ 呼び出された関数
 - ・ 修飾名
 - ・ 行番号

- ・ 新しいテーブルとして、脆弱性メソッドマッチ (vulnerability_method_matches) がレポートデータベースに追加されました。次のカラムがあります。
 - ・ id。ID。
 - ・ project_version_id。到達可能な脆弱性があるプロジェクトバージョンのUUID。
 - ・ vuln_source。脆弱性のソース。脆弱性の影響解析の場合、値はBDSAです。
 - ・ vuln_id。脆弱性ID (BDSA-2020-1234など)。
 - ・ qualified_name。関数が呼び出されるクラスの名前。
 - ・ called_function。コード内で脆弱性を到達可能にする脆弱な関数呼び出しの名前。
 - ・ line_number。コード内で脆弱な関数が呼び出される行番号。
- ・ 脆弱性レポート (脆弱性修正レポート、脆弱性ステータスレポート、および脆弱性更新レポート) には、セキュリティ脆弱性が到達可能か (真)、または到達不能か (偽) を示すために、レポートの末尾に [到達可能] という新しいカラムが追加されました。

構成表の計算情報

Black Duck では、プロジェクトバージョン構成表の計算ステータスに関する詳細情報が提供されるようになりました。

Black Duck UI のプロジェクトバージョンヘッダーにある新しい [ステータス] インジケータ ([コンポーネント] インジケータに代わるもの) は、構成表の現在のステータスを示し、構成表イベントの処理の状態を通知します。更なる情報として、新しい [構成表処理ステータス] ダイアログボックスに、保留中、処理中、または失敗したイベントが表示されます。

Black Duck では、構成表イベントクリーンアップジョブ (VersionBomEventCleanupJob) の頻度も構成できます。このジョブは、処理エラーまたはトポロジ変更によってスタックした可能性のある構成表イベントをクリアします。

ポリシーの機能強化

- ・ ポリシー管理では、次のカスタムフィールドに基づいてポリシールールを作成する機能が提供されます。
 - ・ ブール、日付、ドロップダウン、複数選択、単一選択、テキストの各フィールドタイプ用のコンポーネントカスタムフィールド。
 - ・ ブール、日付、ドロップダウン、複数選択、単一選択、テキストの各フィールドタイプ用のコンポーネントバージョンカスタムフィールド。
- ・ これらの条件のポリシールールを作成する際に、宣言されたライセンスデータとディープ (埋め込み) ライセンスデータを区別できるようになりました。
 - ・ ライセンス
 - ・ ライセンスの有効期限
 - ・ ライセンスファミリ



注:

これらのライセンス条件を使用する既存のポリシールールは、宣言されたライセンスにのみ適用されるようになりました。これらのライセンス条件に対しては、ディープ (埋め込み) ライセンス用に、個別のポリシールールを作成する必要があります。

レポートの機能強化

以前はグローバルレベルまたはプロジェクトレベルでのみ利用可能だった脆弱性レポート (脆弱性修正レポート、脆弱性ステータスレポート、および脆弱性更新レポート) が、プロジェクトバージョンで利用できるようになりました。

スニペットファイルサイズの構成

スニペットでスキャンされるデフォルトの最大ファイルサイズが変更可能になり、1 MBから16 MBまでの値を選択できるようになりました。

マップされていないコードの場所のクリーンアップ構成

Black Duck では、マップされていないコードの場所データを365日ごとにパージします。この機能を無効にして、マップされていないコードの場所データがパージされないようにすることができます。また、定期的にスキャンしてデータを頻繁に破棄するために、保持期間の日数をより短く設定することもできます。

アクセストークン

ユーザーアクセストークンのスコープのオプションは、読み取りまたは読み書きになりました。

サポートされるブラウザのバージョン

- Safariバージョン14.0.1(14610.2.11.51.10)
- Chromeバージョン87.0.4280.88(公式ビルド)(x86_64)
- Firefox 83.0(64ビット)
- Internet Explorer 11 11.630.19041.0

Internet Explorer 11のサポートは廃止されます。Black Duckは、Black Duck 2021.2.0 リリース以降でのInternet Explorer 11のサポートを終了します。

- Microsoft Edge 87.0.664.60(公式ビルド)(64ビット)

コンテナバージョン

- blackducksoftware/blackduck-postgres:1.0.16
- blackducksoftware/blackduck-authentication:2020.12.0
- blackducksoftware/blackduck-webapp:2020.12.0
- blackducksoftware/blackduck-scan:2020.12.0
- blackducksoftware/blackduck-jobrunner:2020.12.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash:1.0.8
- blackducksoftware/blackduck-registration:2020.12.0
- blackducksoftware/blackduck-nginx:1.0.26
- blackducksoftware/blackduck-documentation:2020.12.0
- blackducksoftware/blackduck-upload-cache:1.0.15
- blackducksoftware/blackduck-redis:2020.12.0
- blackducksoftware/blackduck-bomengine:2020.12.0
- sigsynopsys/bdba-worker:2020.09-1
- blackducksoftware/rabbitmq:1.2.2

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2020.10.0が日本語にローカライズされました。

APIの機能強化

- ・ createdAtフィールドでプロジェクト(api/projects)を並べ替える機能が追加されました。
- ・ ある日付の前後に作成されたプロジェクトのapi/projectsエンドポイントにフィルタを適用する機能が追加されました。
- ・ 脆弱性の影響解析機能の一部として、脆弱性マッチを表示するAPIが追加されました。
GET /api/projects/{projectId}/versions/{projectVersionId}/vulnerabilities/{vulnerabilityId}/vulnerability-matches
- ・ 次の構成表エンドポイントが追加されました。
 - ・ 構成表ステータス概要の取得:
GET /api/projects/{projectId}/versions/{projectVersionId}/bom-status
 - ・ 構成表のイベントのリスト:
GET /api/projects/{projectId}/versions/{projectVersionId}/bom-events
 - ・ 失敗した構成表イベントの削除:
DELETE /api/projects/{projectId}/versions/{projectVersionId}/bom-events/{bomEventId}
 - ・ 失敗したすべてのイベントの構成表からの削除:
DELETE /api/projects/{projectId}/versions/{projectVersionId}/bom-events
- ・ 新しいパスワード設定エンドポイント:
 - ・ パスワード設定の取得:
GET /api/password/security/settings
 - ・ システムパスワード設定の取得:
GET /api/password/management/settings
 - ・ システムパスワード設定の更新:
PUT /api/password/management/settings
 - ・ パスワードの検証:
POST /api/password/security/validate
- ・ /api/catalog-risk-profile-dashboard APIは、HTTP 404(Not Found)を返すようになりました。

2020.12.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (Hub-24839)。[コンポーネントの追加/編集]ダイアログボックスで一部のコンポーネントの取得元IDを選択できなかった問題を修正しました。
- ・ (Hub-24911)。KBUpdateJobが失敗してコンポーネントの更新がスキップされていた問題が修正されました。
- ・ (Hub-25230)。ユーザーがライセンステキストを開いたり編集したりする際に、ライセンステキストウィンドウが表示されなかった問題が修正されました。
- ・ (Hub-25452)。[ソース]タブでライセンス検索結果ページを表示した際にライセンスタイプを選択すると、[検出タイプ]フィルタが自動で追加されるように、問題を修正しました。
- ・ (Hub-25489)。サブフォルダが変更されたときに[ソース]タブのフィルタがリセットされていた問題を修正しました。

- ・ (Hub-25603)。別のパスを選択したときに、[スニペットビュー]ダイアログボックスの[ソース]タブにある[マッチしたファイルパス]フィールドに表示されるパスが更新されるように、問題を修正しました。
- ・ (Hub-25681)。汎用/未指定コンポーネントバージョンのライセンスをProtex BOMツールでインポートできなかった問題を修正しました。
- ・ (Hub-25715)。マウスを使用しないと、[カスタムフィールドの管理]ページの[アクティブ]ステータスを変更できなかった問題を修正しました。
- ・ (Hub-25739)。構成表コンポーネントのすべてのコメントを表示できなかった問題が修正されました。
- ・ (Hub-25874)。データが同じカラム名にあるにもかかわらず、bom_component_custom_fields_date_time.csvレポートにcomponents_date_time.csvレポートと異なるデータがリストされていた問題が修正されました。
- ・ (Hub-26442)。プロジェクト所有者がスキャンをプロジェクトバージョン内から削除できなかった問題が修正されました。
- ・ (Hub-26496)。コンポーネントの使用法が変更されたときにライセンスリスクが変更されたにもかかわらず、ライセンスリスクに対するポリシー違反が引き続きトリガーされていた問題が修正されました。

Black Duck 2020.10.x

バージョン2020.10.1の新機能および変更された機能

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:1.0.13
- ・ blackducksoftware/blackduck-authentication:2020.10.1
- ・ blackducksoftware/blackduck-webapp:2020.10.1
- ・ blackducksoftware/blackduck-scan:2020.10.1
- ・ blackducksoftware/blackduck-jobrunner:2020.10.1
- ・ blackducksoftware/blackduck-cfssl:1.0.1
- ・ blackducksoftware/blackduck-logstash:1.0.8
- ・ blackducksoftware/blackduck-registration:2020.10.1
- ・ blackducksoftware/blackduck-nginx:1.0.26
- ・ blackducksoftware/blackduck-documentation:2020.10.1
- ・ blackducksoftware/blackduck-upload-cache:1.0.15
- ・ blackducksoftware/blackduck-redis:2020.10.1
- ・ sigsynopsys/bdba-worker:2020.09-1
- ・ blackducksoftware/rabbitmq:1.2.2

2020.10.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (Hub-25489)。別のフォルダを選択したときに[ソース]タブで選択されているフィルタがリセットされていた問題を修正しました。
- ・ (Hub-25515)。ホストインスタンスでTLS 1.3が動作している場合に、アップロード時に署名スキャナが失敗し、エラーメッセージ「エラー:ホストへの接続を保護できません」が表示される問題が修正されました。

- ・ (Hub-25791)。バージョン2020.4.2からバージョン2020.6.1/2020.6.2にアップグレードした後に、スキャンにかかる時間が大幅に増加していた問題が修正されました。
- ・ (Hub-26027)。Black Duckで次のエラー メッセージが表示されていた問題を修正しました。「エラー: アプリケーションに不明なエラーが発生しました。(正しくないリクエスト)エラー。error.[core.rest.common_error]が、Black Duck Detectスキャンのアップロード時にBlack Duckに表示されていた問題が修正されました。
- ・ (Hub-26085)。バイナリスキャンで2番目の空のスキャンが追加されていた問題が修正されました。

バージョン2020.10.0の発表

2020.12.0リリースまで延期された新しいコンテナとシステム要件の変更


Black Duck は以前、2020.10.0リリース向けに、BOM EngineおよびRabbitMQ (現在は必須コンテナ) という2つのコンテナが追加されると発表しました。この要件は、2020.12.0リリースに延期されました。

2020.12.0リリースでは、すべてのコンテナの単一インスタンスを実行するための最小システム要件は次のようになります。

- ・ 6 CPU
- ・ Redisの最小構成の場合は26 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は29 GB RAM
- ・ データベースおよびその他のBlack Duckコンテナ用に250 GBの空きディスク容量
- ・ データベースバックアップに適した容量

2020.12.0リリースでは、Black Duck - Binary AnalysisでBlack Duckを実行するために必要とされる最小ハードウェアは次のようになります。

- ・ 7 CPU
- ・ Redisの最小構成の場合は30 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は33 GB RAM
- ・ データベースおよびその他のBlack Duckコンテナ用に350 GBの空きディスク容量
- ・ データベースバックアップに適した容量

 注: binaryscannerコンテナを1個追加することにより、1 CPU、2 GB RAM、100 GBの空きディスク容量の追加が必要になります。

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2020.8.0が日本語にローカライズされました。

バージョン2020.10.0の新機能および変更された機能

新しいカスタムコンポーネントダッシュボード

2020.10.0では、コンポーネントダッシュボードが、保存済みコンポーネント検索を使用できるカスタムコンポーネントダッシュボードに切り替わり、重要なコンポーネントバージョンを簡単に表示できるようになりました。Black Duck では、さまざまな属性を使用してプロジェクト内で使用されるコンポーネントを検索し、検索を保存してから、この[ダッシュボード]ページを使用して保存済み検索からダッシュボードを表示できるようになりました。

カスタムコンポーネントダッシュボードでは、コンポーネントバージョンごとに次の情報が表示されます。

- ・ 当該コンポーネントバージョンを使用しているプロジェクトバージョンの数、および各プロジェクトバージョンのフェーズ、ライセンス、レビューステータス、セキュリティ上のリスク

- ・ リスクカテゴリ別の脆弱性の数
- ・ ライセンスおよび運用上のリスク
- ・ ポリシー違反
- ・ 承認済みステータス
- ・ 当該コンポーネントバージョンが最初に検出された日付
- ・ Black Duck KnowledgeBaseに基づく、コンポーネントがリリースされた日付
- ・ 新しいバージョンの数
- ・ このコンポーネントの脆弱性が最後に更新された日時

コンポーネントおよびBlack Duck KnowledgeBase検索の機能強化

コンポーネントの検索は、コンポーネントの検索に使用できる属性と、検索結果に表示される情報によって強化されています。プロジェクトで使用されるコンポーネント検索とBlack Duck KnowledgeBaseでのコンポーネント検索を簡単に区別できるように、UIも機能強化されました。

Black Duck KnowledgeBase検索の検索属性は変更されていませんが、Black Duckプロジェクトで使用されているコンポーネントバージョンを検索する場合に、次の属性を使用できます。

- ・ セキュリティ上のリスク
- ・ ライセンスリスク
- ・ 運用上のリスク
- ・ ポリシールール
- ・ ポリシー違反の重大度
- ・ レビューステータス
- ・ コンポーネントの承認済みステータス
- ・ 最初の検出
- ・ ライセンスファミリー
- ・ カスタムフィールドデータがない
- ・ リリース日
- ・ ライセンス
- ・ 脆弱性CWE
- ・ 脆弱性報告日

検索条件に一致するコンポーネントバージョンごとに、次の情報が表示されます。

- ・ 当該コンポーネントバージョンを使用しているプロジェクトバージョンの数、および各プロジェクトバージョンのフェーズ、ライセンス、レビューステータス、セキュリティ上のリスク
- ・ リスクカテゴリ別の脆弱性の数
- ・ ライセンスおよび運用上のリスク
- ・ ポリシー違反
- ・ 承認済みステータス
- ・ 当該コンポーネントバージョンが最初に検出された日付
- ・ Black Duck KnowledgeBaseに基づく、コンポーネントがリリースされた日付

- ・ 新しいバージョンの数
- ・ このコンポーネントの脆弱性が最後に更新された日時

これらのコンポーネントは、前述のように、検索結果を保存して[ダッシュボード]ページに表示できるようになりました。

ナレッジベースコンポーネント検索結果ごとに、次の情報が表示されます。


- ・ 当該コンポーネントを使用しているプロジェクトバージョンの数、各プロジェクトバージョンのリスト、フェーズ、使用されているコンポーネントバージョン、関連するセキュリティ上のリスク
- ・ コミットアクティビティ推移
- ・ 最終コミット日
- ・ コンポーネントバージョンの数
- ・ このコンポーネントのタグ

保存済み検索の機能強化

Black Duck [ダッシュボード]ページでは、保存済み検索をフィルタにかけたり並べ替えたりできるようになりました。

ライセンスの競合

Black Duckの2020.10.0リリースでは、齟齬があるカスタム ライセンス条項を指定できるようになりました。Black Duck KnowledgeBase条項またはユーザーのカスタムライセンス条項と競合している禁止/必須アクションに対しては、カスタムのライセンス条項を定義できます。

 注：現在、プロジェクトバージョン構成表では、齟齬があるライセンス条項を表示することはできません。この機能は、今後のBlack Duckリリースで利用可能になる予定です。

ライセンス管理の機能強化

次の新しい3つのフィルタが、[ライセンス管理]の[ライセンス条項]タブに追加されました。

- ・ ライセンスに関連付けられている
- ・ 齟齬がある条項が含まれている
- ・ 責任

新しいコンポーネントの使用状況

Black Duck は、コンポーネントの使用状況を調べる必要があることを示すためにユーザーが使用できる使用法[未指定]を追加しました。[動的にリンク]などの既存のデフォルト値の代わりに、この使用法をデフォルト値として使用すると便利な場合があります。この場合、コンポーネントに正しい使用法値またはデフォルト値が割り当てられているかどうかの混乱が解消されます。

新しい階層

Black Duck は、最重要階層として指定できる階層0を追加しました。

この新しい階層により、次のデフォルトポリシールールが階層0を含むように変更されました。

- ・ 脆弱性が高1よりも大きい外部階層0、階層1、または階層2プロジェクトなし
- ・ 脆弱性が中3よりも大きい外部階層0、階層1、または階層2プロジェクトなし

既存の階層に変更はありません。

カスタムフィールドの機能強化

カスタムフィールドに対して、次の機能拡張が行われました

- ・ Black Duck で、カスタムフィールドが必須であることを示す機能が追加されました。
 - ・ カスタムフィールド情報を表示すると、警告メッセージ「*その他のフィールドは必須です」が表示されます。ただし、必須のカスタムフィールドにデータが入力されていない場合でも、ユーザーは、カスタム以外のフィールド情報と必須以外のカスタムフィールドの情報をページで表示したり保存したりできます。
 - ・ 情報が欠落しているプロジェクトバージョン構成表内のコンポーネントを表示できるように、新しいフィルタ[カスタムフィールドデータがない]が構成表に追加されました。
- ・ ブール型や単一選択フィールドタイプで、カスタムフィールド情報を表示する際にも、選択を解除できるオプションが追加されました。

許可された署名リスト

スキャンしたコードに含まれるオープン ソース ソフトウェアを判定するために、署名リストで、Black DuckがBlack Duck KnowledgeBase Webサービスに送信する署名を定義します。署名スキャナ に、新しい2つのパラメータが追加されました。このパラメータを使用して、バイナリファイル拡張子またはソースファイル拡張子の許可された署名リストを作成できます。各リストはオプションであり、他のリストとは独立して動作します。

- ・ `--BinaryAllowedList x, y, z` (x, y, zは、SHA-1 (バイナリ) ファイルの承認済みファイル拡張子です)
- ・ `--SourceAllowedList a, b, c` (a, b, cは、クリーンなSHA-1 (ソースコード) ファイルの承認済みファイル拡張子です)

脆弱性の影響解析の機能強化

脆弱性の影響解析に対して、次の機能強化が行われました。

- ・ セキュリティ脆弱性が到達可能(真)であるか到達不能(偽)であるかを示すために、`security_date_time.csv` プロジェクトバージョンレポートの最後に新しい列[到達可能]が追加されました。
- ・ 新しいフィルタ[到達可能]がプロジェクトバージョンの[セキュリティ]タブに追加されました。

レポートの機能強化

次のレポート機能が強化されました。

- ・ `components_date_time.csv` プロジェクトバージョンレポートの最後に新しい列[コメント]が追加され、各コンポーネントのコメントが一覧表示されるようになりました。
- ・ マッチタイプを判定するために、`vulnerability-status-report_date_time.csv` レポートの最後に新しい列[マッチタイプ]が追加されました。

レポートデータベースの機能強化

次のカラムがコンポーネントマッチ表 (`component_matches`) に追加されました。

- ・ `match_confidence`。スニペット、バイナリ、または部分的なファイルマッチを除いたうえで、マッチの信頼性を表します。
- ・ `match_archive_context`。プロジェクトのルートディレクトリを基準とした、アーカイブ済みファイルへのローカルパスです。
- ・ `snippet_confirmation_status`。スニペットマッチのステータスをレビューします。

HTTP/2およびTLS 1.3

ブラウザに表示されるBlack Duck UIのセキュリティとレンダリングを改善するために、Black Duckは、Black Duck NGINX WebサーバーでHTTP/2およびTLS 1.3をサポートするようになりました。Black Duck NGINXウェブサーバーは、HTTP/1.1およびTLS 1.2も引き続きサポートします。

スキャンページのためのジョブに対する変更

BomVulnerabilityNotificationJobとLicenseTermFulfillmentJobでも、古い監査イベントが削除されました。

サポートされるブラウザのバージョン

- ・ Safariバージョン13.1.2 (14609.3.5.1.5)
- ・ Chromeバージョン86.0.4240.80
- ・ Firefox 82 (64ビット)
- ・ Internet Explorer 11.572.19041.0

Internet Explorer 11のサポートは廃止されます。Black Duckは、Black Duck 2021.2.0 リリース以降でのInternet Explorer 11のサポートを終了します。

- ・ Microsoft Edge 86.0.622.51 (公式ビルド) (64ビット)

コンテナバージョン

- ・ blackducksoftware/blackduck-postgres:1.0.13
- ・ blackducksoftware/blackduck-authentication:2020.10.0
- ・ blackducksoftware/blackduck-webapp:2020.10.0
- ・ blackducksoftware/blackduck-scan:2020.10.0
- ・ blackducksoftware/blackduck-jobrunner:2020.10.0
- ・ blackducksoftware/blackduck-cfssl:1.0.1
- ・ blackducksoftware/blackduck-logstash:1.0.6
- ・ blackducksoftware/blackduck-registration:2020.10.0
- ・ blackducksoftware/blackduck-nginx:1.0.26
- ・ blackducksoftware/blackduck-documentation:2020.10.0
- ・ blackducksoftware/blackduck-upload-cache:1.0.15
- ・ blackducksoftware/blackduck-redis:2020.10.0
- ・ sigsynopsys/bdba-worker:2020.09
- ・ blackducksoftware/rabbitmq:1.2.2

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2020.8.0が日本語にローカライズされました。

APIの機能強化

- ・ Black Duckのシングルサインオン (SSO) ステータスを確認するためのエンドポイントが追加されました。
GET /api/sso/status

- ・ SAML/LDAP構成を取得するためのエンドポイントが追加されました(管理者専用)。
 - ・ SSO構成の読み取り:
GET /api/sso/configuration
 - ・ IDPメタデータファイルのダウンロード:
GET /api/sso/idp-metadata
 - ・ また以下のSSOエンドポイントも追加されました。
 - ・ SSO構成の更新:
POST /api/sso/configuration
 - ・ IDPメタデータファイルのアップロード:
POST /api/sso/idp-metadata
- ・ 次の構成表階層型コンポーネントエンドポイントが追加されました。
 - ・ 階層型ルートコンポーネントのリスト:
GET /api/projects/{projectId}/versions/{projectVersionId}/hierarchical-components
 - ・ 階層型子コンポーネントのリスト:
GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/hierarchical-components/{hierarchicalId}/children
 - ・ 階層型子コンポーネントバージョンのリスト:
GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/hierarchical-components/{hierarchicalId}/children
- ・ 脆弱性の通知APIに新しいフィールドが追加され、通知をさらに分類できるようになりました。これらの通知には、構成表で変更された脆弱性情報が含まれ、次のフィールドが含まれます。
 - ・ vulnerabilityNotificationCause
発生し、通知をトリガーした脆弱性イベントの種類についての情報。脆弱性の追加/削除、コメントの変更、修正の詳細の変更、脆弱性の重大度の変更、ステータスの変更などです。
 - ・ eventSource
通知を生成したソースの情報。スキャン、Black Duck KB更新、ユーザーアクション(修正、優先順位の変更、調整)などです。
- ・ /api/catalog-risk-profile-dashboard APIは、HTTP 410(GONE)を返すようになりました。

2020.10.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ・ (Hub-20559, 22100)。異なるルートディレクトリから同じコードの場所をスキャンしたとき、またはプロジェクトバージョンを複製したときに、スニペットの調整が失われていた問題が修正されました。
- ・ (Hub-21421)。大規模プロジェクトで印刷機能が動作しなかった問題が修正されました。
- ・ (Hub-23705, 25560)。ユーザーが作成したレポートをユーザーが削除できなかった問題が修正されました。
- ・ (Hub-23709)。スキャン時に次のscan.cli.sh警告メッセージが表示されていた問題が修正されました。「すべてのマニフェストからマニフェストを検出できません」
- ・ (Hub-24330)。ProtexプロジェクトをBlack Duckバージョン2019.10.3にインポートしようすると、エラーメッセージ「キー値の重複は一意の制約に違反しています」が表示されていた問題が修正されました。

- ・ (Hub-24673)。コンポーネント数が32,000を超えていると、[ダッシュボード]ページから移動するときに失敗していた問題を修正しました。
- ・ (Hub-24675)。root_bom_consumer_node_idが正しく設定されていなかった問題が修正されました。
- ・ (Hub-24871)。リリース2019.10.0以降のPostgreSQLデータベースの拡張に関する問題が修正されました。
- ・ (Hub-24772)。構成表印刷時のデフォルト.pdfファイル名がプロジェクト名とバージョン名でなかった問題が修正されました。
- ・ (Hub-24839)。[コンポーネントの追加/編集]ダイアログボックスで一部のコンポーネントの取得元IDを選択できなかった問題を修正しました。
- ・ (Hub-24947)。構成表にプロジェクトを追加した際に、検索結果の表示で一貫性が損なわれていた問題が修正されました。
- ・ (Hub-25171)。APIを使用して修正した場合に、再スキャン (PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/origins/{originId}/vulnerabilities/{vulnerabilityId}/remediation) するまで、脆弱性の件数が更新されなかった問題が修正されました。
- ・ (Hub-25219)。APIを使用してレポートを作成する際の問題(localeに指定したja_JPが無視されるなど、locale指定時の問題)が修正されました。生成レポートの言語は、localeフィールドで正しく設定されるようになりました。
- ・ (Hub-25234)。構成表を印刷する[印刷]ボタンに、バーグラフのカウン트가表示されないことがあった問題を修正しました。
- ・ (Hub-25240)。ブラウザまたはAPIが特定の脆弱性(BDSA-2020-1674)の呼び出しで失敗していた問題が修正されました。
- ・ (Hub-25241)。VersionBomComputationJobが次のエラーメッセージでスキャンに失敗していた問題が修正されました。「データ整合性違反 (Constraint: not_null, Detail: on column source_start_lines)」。
- ・ (Hub-25244)。Black Duckリリース2020.4.2にアップグレードした後に、手動で追加したコンポーネントが構成表から削除されていた問題が修正されました。
- ・ (Hub-25247)。Black Duck PostgreSQLログに、次のエラーメッセージが表示されていた問題が修正されました。エラー: キー値の重複は一意の制約「scan_component_scan_id_bdio_node_id_key」に違反しています。
- ・ (Hub-25321)。構成表ページをスクロールすると、テキストを表示すべきでないページ領域にテキストが表示されていた問題が修正されました。
- ・ (Hub-25324)。[スキャン名]ページで、ワードラップが行われていなかった問題を修正しました。
- ・ (Hub-25478)。[セキュリティ]ページのセキュリティリスクフィルタが表示されなかった問題が修正されました。
- ・ (Hub-25508)。以前のメディアタイプ (v4およびv5) がポリシールールAPI (GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/policy-rules) に対して機能しないことがあった問題が修正されました。
- ・ (Hub-25522、25523)。Chrome for Black Duckバージョン2020.8.0の構成表印刷プレビューウィンドウで発生していた表示形式の問題が修正されました。
- ・ (Hub-25548)。階層ビューで新しいコンポーネントマッチを選択しても、ソースビューのコンポーネントマッチが更新されなかった問題が修正されました。
- ・ (Hub-25570)。[セキュリティダッシュボード]ページで一部の領域が読み込まれなかった問題が修正されました。
- ・ (Hub-25608)。脆弱性更新レポートの[新しい脆弱性]および[新たに修正された脆弱性]カテゴリで、脆弱性が2回カウントされていた問題が修正されました。
- ・ (Hub-25649)。[ダッシュボード]ページのポリシー違反ポップアップウィンドウが閉じなかった問題が修正されました。

2. Previous Releases · Black Duck 2020.10.x

- ・ (Hub-25841)。テキストデータ型のカスタムフィールドに入力した数値が日付形式に変換されていた問題が修正されました。

3. 既知の問題と制限事項

Black Duckの既知の問題と制限事項は次のとおりです。

新しい既知の問題

- ・ 現在、Bitbucket Data Center用のSCM統合が正しく機能していません。この機能の使用についてのお問い合わせは、Black Duckサポートまでご連絡ください。
- ・ Bitbucket Cloud SCMプロバイダーのユーザーは、ワークスペースからリポジトリをクローンするために、Bitbucketで同じワークスペース名とワークスペースIDを使用する必要があります。
- ・ [検索]ページでCISA既知の悪用された脆弱性を検索する場合は、結果を取得するために[影響を与えるプロジェクト]のチェックボックスもオンにする必要があります。[CISA既知の悪用された脆弱性]のチェックボックスをオンにただけでは、検索結果は得られません。

現在の既知の問題と制限事項

- ・ [管理者] > [診断] > [ヒートマップ]の下にある[スキャンヒートマップ]に、ローカル時間ではなくUTC時間で結果が表示されます。この新機能を使用する場合は、この点に注意してください。
- ・ マッチスコアのしきい値設定で削除対象とマークされたコンポーネントは、UIでBDIOを再アップロードするときには削除されません。
- ・ [アーカイブ済みプロジェクトバージョンのマッチしないスキャンファイルデータのみをパージする]および[マッチしないすべてのファイルデータをパージする]リンクは、プロジェクト([プロジェクト] > [設定]タブ)とグローバル([管理者] > [システム設定] > [データ保持])の両方のレベルで機能しません
- ・ ユーザーの認証にLDAPディレクトリサーバーを使用している場合は、次の点を考慮してください。
 - ・ Black Duck は、単一のLDAPサーバーをサポートしています。複数のサーバーはサポートされていません。
 - ・ ユーザーがディレクトリサーバーから削除されても、Black Duckユーザーアカウントはアクティブと表示され続けます。ただし、認証情報は有効ではなくなり、ログインに使用できません。
 - ・ グループがディレクトリサーバーから削除されても、Black Duckグループは削除されません。グループは手動で削除してください。
- ・ タグ付けでは、文字、数字、プラス(+)および下線(_)のみがサポートされています。
- ・ Black Duckがユーザーを認証している場合、ログイン中にユーザー名の大文字と小文字は区別されません。LDAPユーザー認証が有効になっている場合、ユーザー名の大文字と小文字は区別されます。
- ・ コードの場所に大規模な構成表がある場合、コードの場所を削除すると、ユーザーインターフェイスのタイムアウトエラーで失敗することがあります。