

Black Duck SCA Release Notes

Black Duck SCA 2026.7.2

Copyright ©2026 by Black Duck.

All rights reserved. All use of this documentation is subject to the license agreement between Black Duck Software, Inc. and the licensee. No part of the contents of this document may be reproduced or transmitted in any form or by any means without the prior written permission of Black Duck Software, Inc.

Black Duck, Know Your Code, and the Black Duck logo are registered trademarks of Black Duck Software, Inc. in the United States and other jurisdictions. Black Duck Code Center, Black Duck Code Sight, Black Duck Hub, Black Duck Protex, and Black Duck Suite are trademarks of Black Duck Software, Inc. All other trademarks or registered trademarks are the sole property of their respective owners.

03-11-2026

Contents

Preface....6
Black Duck documentation....6
Customer support....6
Black Duck Community....7
Training....7
Black Duck Statement on Inclusivity and Diversity....7
Black Duck Security Commitments....8

1. Black Duck SCA 2026.7.2....9
Announcements....9
New and Changed Features....9
API Enhancements....10
Binary Scanner Information....10
Fixed Issues....10

2. Previous Black Duck SCA Releases....11
Black Duck SCA 2026.7.x....11
Black Duck SCA 2026.7.1....11
Black Duck SCA 2026.7.0....13
Black Duck SCA 2026.4.x....19
Black Duck SCA 2026.4.2....19
Black Duck SCA 2026.4.1....20
Black Duck SCA 2026.4.0....22
Black Duck SCA 2026.1.x....27
Black Duck SCA 2026.1.2....27
Black Duck SCA 2026.1.1....28
Black Duck SCA 2026.1.0....30
Black Duck SCA 2025.10.x....36
Black Duck SCA 2025.10.2....36
Black Duck SCA 2025.10.1....37
Black Duck SCA 2025.10.0....39
Black Duck SCA 2025.7.x....48
Black Duck SCA 2025.7.1....48
Black Duck SCA 2025.7.0....49
Black Duck SCA 2025.4.x....58
Black Duck SCA 2025.4.2....58
Black Duck SCA 2025.4.1....60
Black Duck SCA 2025.4.0....61
Black Duck SCA 2025.1.x....68
Black Duck 2025.1.1....68
Black Duck SCA 2025.1.0....71
Black Duck SCA 2024.10.x....75
Black Duck 2024.10.1....75
Black Duck SCA 2024.10.0....78
Black Duck SCA 2024.7.x....85
Black Duck 2024.7.3....85

Black Duck SCA 2024.7.2 ... 86
Black Duck SCA 2024.7.1 ... 87
Black Duck SCA 2024.7.0 ... 90
Black Duck SCA 2024.4.x ... 97
Black Duck SCA 2024.4.1 ... 97
Black Duck SCA 2024.4.0 ... 99
Black Duck SCA 2024.1.x ... 105
Black Duck 2024.1.1 ... 105
Black Duck SCA 2024.1.0 ... 108
Black Duck SCA 2023.10.x ... 113
Black Duck version 2023.10.2 ... 113
Black Duck version 2023.10.1 ... 115
Black Duck version 2023.10.0 ... 117
Black Duck SCA 2023.7.x ... 127
Black Duck version 2023.7.3 ... 127
Black Duck version 2023.7.2 ... 128
Black Duck Version 2023.7.1 ... 129
Black Duck version 2023.7.0 ... 134
Black Duck SCA 2023.4.x ... 140
Black Duck version 2023.4.2 ... 140
Black Duck version 2023.4.1 ... 141
Black Duck version 2023.4.0 ... 142
Black Duck SCA 2023.1.x ... 150
Black Duck version 2023.1.2 ... 150
Black Duck version 2023.1.1 ... 152
Black Duck version 2023.1.0 ... 152
Black Duck SCA 2022.10.x ... 159
Black Duck version 2022.10.3 ... 159
Black Duck version 2022.10.2 ... 159
Black Duck version 2022.10.1 ... 161
Black Duck version 2022.10.0 ... 162
Black Duck SCA 2022.7.x ... 171
Announcements for Version 2022.7.2 ... 171
New and changed features in version 2022.7.2 ... 171
Announcements for Version 2022.7.1 ... 172
New and changed features in version 2022.7.1 ... 172
Announcements for Version 2022.7.0 ... 175
New and Changed Features in Version 2022.7.0 ... 177
Black Duck SCA 2022.4.x ... 183
New and Changed Features in Version 2022.4.2 ... 183
New and Changed Features in Version 2022.4.1 ... 184
Announcements for Version 2022.4.0 ... 186
New and Changed Features in Version 2022.4.0 ... 189
Black Duck SCA 2022.2.x ... 194
New and Changed Features in Version 2022.2.2 ... 194
New and Changed Features in Version 2022.2.1 ... 195
Announcements for Version 2022.2.0 ... 197
New and Changed Features in Version 2022.2.0 ... 199
Black Duck SCA 2021.10.x ... 210
Announcements for Version 2021.10.3 ... 210
New and Changed Features in Version 2021.10.3 ... 211
Announcements for Version 2021.10.2 ... 211
New and Changed Features in Version 2021.10.2 ... 212
New and Changed Features in Version 2021.10.1 ... 212

Announcements for Version 2021.10.0 214
New and Changed Features in Version 2021.10.0 216
Black Duck SCA 2021.8.x 221
New and Changed Features in Version 2021.8.8 221
Announcements for Version 2021.8.7 221
New and Changed Features in Version 2021.8.7 222
Announcements for Version 2021.8.6 223
New and Changed Features in Version 2021.8.6 223
New and Changed Features in Version 2021.8.5 224
New and Changed Features in Version 2021.8.4 224
New and Changed Features in Version 2021.8.3 225
New and Changed Features in Version 2021.8.2 226
New and Changed Features in Version 2021.8.1 227
Announcements for Version 2021.8.0 228
New and Changed Features in Version 2021.8.0 228
Black Duck SCA 2021.6.x 233
New and Changed Features in Version 2021.6.2 233
New and Changed Features in Version 2021.6.1 234
Announcements for Version 2021.6.0 235
New and Changed Features in Version 2021.6.0 236
Black Duck SCA 2021.4.x 242
New and Changed Features in Version 2021.4.1 242
Announcements for Version 2021.4.0 242
New and Changed Features in Version 2021.4.0 244
Black Duck SCA 2021.2.x 250
New and Changed Features in Version 2021.2.1 250
Announcements for Version 2021.2.0 251
New and Changed Features in Version 2021.2.0 251
Black Duck SCA 2020.12.x 258
Announcements for Version 2020.12.0 258
New and Changed Features in Version 2020.12.0 259
Black Duck SCA 2020.10.x 264
New and Changed Features in Version 2020.10.1 264
Announcements for Version 2020.10.0 265
New and Changed Features in Version 2020.10.0 265

3. Known Issues and Limitations 272

Preface

Black Duck documentation

The documentation for Black Duck consists of online help and these documents:

Title	File	Description
Release Notes	release_notes.pdf	Contains information about the new and improved features, resolved issues, and known issues in the current and previous releases.
Installing Black Duck using Docker Swarm	install_swarm.pdf	Contains information about installing and upgrading Black Duck using Docker Swarm.
Installing Black Duck using Kubernetes	install_kubernetes.pdf	Contains information about installing and upgrading Black Duck using Kubernetes.
Installing Black Duck using OpenShift	install_openshift.pdf	Contains information about installing and upgrading Black Duck using OpenShift.
Getting Started	getting_started.pdf	Provides first-time users with information on using Black Duck.
Scanning Best Practices	scanning_best_practices.pdf	Provides best practices for scanning.
Getting Started with the SDK	getting_started_sdk.pdf	Contains overview information and a sample use case.
Report Database	report_db.pdf	Contains information on using the report database.
User Guide	user_guide.pdf	Contains information on using Black Duck's UI.

The installation methods for installing Black Duck software in a Kubernetes or OpenShift environment are Helm. Click the following links to view the documentation.

- Helm is a package manager for Kubernetes that you can use to install Black Duck. Black Duck supports Helm3 and the minimum version of Kubernetes is 1.13.

Black Duck integration documentation is available on:

- https://sig-product-docs.blackduck.com/bundle/detect/page/integrations/integrations.html
- https://docs.blackduck.com/p/bridgeintegrations

Customer support

If you have any problems with the software or the documentation, please contact Black Duck Customer Support:

- Online: https://community.blackduck.com/s/contactsupport
- To open a support case, please log in to the Black Duck Community site at https://community.blackduck.com/s/contactsupport.
- Another convenient resource available at all times is the online Community portal.

Black Duck Community

The Black Duck Community is our primary online resource for customer support, solutions, and information. The Community allows users to quickly and easily open support cases and monitor progress, learn important product information, search a knowledgebase, and gain insights from other Black Duck customers. The many features included in the Community center around the following collaborative actions:

- Connect – Open support cases and monitor their progress, as well as, monitor issues that require Engineering or Product Management assistance
- Learn – Insights and best practices from other Black Duck product users to allow you to learn valuable lessons from a diverse group of industry leading companies. In addition, the Customer Hub puts all the latest product news and updates from Black Duck at your fingertips, helping you to better utilize our products and services to maximize the value of open source within your organization.
- Solve – Quickly and easily get the answers you're seeking with the access to rich content and product knowledge from Black Duck experts and our Knowledgebase.
- Share – Collaborate and connect with Black Duck staff and other customers to crowdsource solutions and share your thoughts on product direction.

Access the Customer Success Community. If you do not have an account or have trouble accessing the system, click here to get started, or send an email to community.manager@blackduck.com.

Training

Black Duck Customer Education is a one-stop resource for all your Black Duck education needs. It provides you with 24x7 access to online training courses and how-to videos.

New videos and courses are added monthly.

In Black Duck Education, you can:

- Learn at your own pace.
- Review courses as often as you wish.
- Take assessments to test your skills.
- Print certificates of completion to showcase your accomplishments.

Learn more at https://blackduck.skilljar.com/page/black-duck or for help with Black Duck, select **Black Duck Tutorials** from the Help menu () in the Black Duck UI.

Black Duck Statement on Inclusivity and Diversity

Black Duck is committed to creating an inclusive environment where every employee, customer, and partner feels welcomed. We are reviewing and removing exclusionary language from our products and supporting customer-facing collateral. Our effort also includes internal initiatives to remove biased language from our

engineering and working environment, including terms that are embedded in our software and IPs. At the same time, we are working to ensure that our web content and software applications are usable to people of varying abilities. You may still find examples of non-inclusive language in our software or documentation as our IPs implement industry-standard specifications that are currently under review to remove exclusionary language.

Black Duck Security Commitments

As an organization dedicated to protecting and securing our customers' applications, Black Duck is equally committed to our customers' data security and privacy. This statement is meant to provide Black Duck customers and prospects with the latest information about our systems, compliance certifications, processes, and other security-related activities.

This statement is available at: Security Commitments | Black Duck

1. Black Duck SCA 2026.7.2

- Announcements
- New and changed features
- API enhancements
- Binary scanner information
- Fixed issues

Announcements

There are no announcements for Black Duck SCA 2026.7.2.

New and Changed Features

There are no new or changed features in Black Duck SCA 2026.7.2.

Container versions

- blackducksoftware/blackduck-postgres:16-2.10
- blackducksoftware/blackduck-postgres-upgrader:16-1.5
- blackducksoftware/blackduck-postgres-waiter:1.0.21
- blackducksoftware/blackduck-cfssl:1.0.38
- blackducksoftware/blackduck-nginx:2026.7.2
- blackducksoftware/blackduck-logstash:1.0.48
- blackducksoftware/bdba-worker:2026.6.3
- blackducksoftware/rabbitmq:1.2.52
- blackducksoftware/blackduck-authentication:2026.7.2
- blackducksoftware/blackduck-bomengine:2026.7.2
- blackducksoftware/blackduck-documentation:2026.7.2
- blackducksoftware/blackduck-integration:2026.7.2
- blackducksoftware/blackduck-jobrunner:2026.7.2
- blackducksoftware/blackduck-redis:2026.7.2
- blackducksoftware/blackduck-registration:2026.7.2
- blackducksoftware/blackduck-scanmatch:2026.7.2
- blackducksoftware/blackduck-storage:2026.7.2
- blackducksoftware/blackduck-webapp:2026.7.2

API Enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck SCA.

There are no API changes in Black Duck SCA 2026.7.2.

Binary Scanner Information

The binary scanner has been updated to version **2026.6.3**.

Fixed Issues

The following customer-reported issues have been fixed in this release:

- (HUB-49112). Fixed an issue where clicking the *N Matches* link in the **Source** column on the BOM tab opened the Source tab but failed to display the corresponding matching source files.
- (HUB-49127). Fixed an issue where users assigned project permissions through project groups or user groups were unable to use the **Bulk Edit** option on project versions because the option was disabled unless the user held global administrator permissions.

2. Previous Black Duck SCA Releases

Black Duck SCA 2026.7.x

Black Duck SCA 2026.7.1

Announcements

There are no announcements for Black Duck SCA 2026.7.1.

New and Changed Features

There are no new or changed features in Black Duck SCA 2026.7.1.

Container versions

- blackducksoftware/blackduck-postgres:16-2.10
- blackducksoftware/blackduck-postgres-upgrader:16-1.5
- blackducksoftware/blackduck-postgres-waiter:1.0.21
- blackducksoftware/blackduck-cfssl:1.0.38
- blackducksoftware/blackduck-nginx:2026.7.1
- blackducksoftware/blackduck-logstash:1.0.48
- blackducksoftware/bdba-worker:2026.6.3
- blackducksoftware/rabbitmq:1.2.52
- blackducksoftware/blackduck-authentication:2026.7.1
- blackducksoftware/blackduck-bomengine:2026.7.1
- blackducksoftware/blackduck-documentation:2026.7.1
- blackducksoftware/blackduck-integration:2026.7.1
- blackducksoftware/blackduck-jobrunner:2026.7.1
- blackducksoftware/blackduck-redis:2026.7.1
- blackducksoftware/blackduck-registration:2026.7.1
- blackducksoftware/blackduck-scanmatch:2026.7.1
- blackducksoftware/blackduck-storage:2026.7.1
- blackducksoftware/blackduck-webapp:2026.7.1

API Enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck SCA.

There are no API changes in Black Duck SCA 2026.7.1.

Binary Scanner Information

The binary scanner has been updated to version **2026.6.3**.

Fixed Issues

The following customer-reported issues have been fixed in this release:

- (HUB-47462). Fixed an issue where a user who was previously set as a project owner or who originally created the project did not appear in the assignable project owner dropdown in **Project Settings > Project Details**.
- (HUB-47780). Fixed an issue where users assigned the Project Manager role who also possessed the Global Project Creator role were erroneously permitted to assign arbitrary project roles when adding users to a project.
- (HUB-47795, HUB-48744). Fixed an issue where updating vulnerability remediation via the LTS Remediation API (`PUT /api/lts-projects/.../remediation`) failed to persist the `remediationStatus` for CVE-primary vulnerability entries that had linked BDSAs.
- (HUB-47891). Fixed an inconsistency on the Project BOM page where vulnerability entries prioritized BDSA over CVE even when the system security ranking was configured to prioritize NVD over BDSA.
- (HUB-48058). Fixed an issue where exporting a BOM to SPDX (versions 2.3 and 3.0) did not format specific component usage types (such as *Implementation of a Standard* and *Dev. Tool / Excluded*) correctly, causing them to revert to default values upon re-import.
- (HUB-48059). Fixed an issue where the `/api/projects/{projectId}/versions/{projectVersionId}/review-components` endpoint ignored `limit` and `offset` pagination parameters when queried with the `bomMatchReviewType:unmatched` filter.
- (HUB-48223). Fixed an issue where the **Updated** timestamp for projects displayed on the Dashboard was not refreshed after project setting modifications, rescans, or BOM updates.
- (HUB-48225). Fixed an issue in Match Review where attempting to confirm a component match that contained multiple origins failed with an HTTP 412 error.
- (HUB-48228). Fixed an issue where changing the version or origin of a manually identified component on the BOM tab resulted in an HTTP 404 error and caused the component to be unintentionally deleted after refreshing the page.
- (HUB-48232). Fixed an issue where navigating to the Source tab on certain project versions resulted in an `undefined` project ID error in the API request URL, preventing source BOM entries from loading.
- (HUB-48248). Fixed an issue in the reporting database where `scan_stats_view` populated empty `user_id` values for code locations containing archived scan entries.
- (HUB-48250). Fixed an issue where snippets marked as ignored unexpectedly reappeared in exported SBOM reports.
- (HUB-48260). Fixed an edge case on the BOM page where distinct components sharing identical names were omitted from the component list when pagination limits were applied.
- (HUB-48371). Fixed an issue where vulnerabilities from deeply nested subprojects were not rolled up transitively or displayed at the top-level parent project view.
- (HUB-48416). Fixed an issue where multiple instances of the on-demand `KbUpdateWorkflowJob-Component Version Security Update` job were queued and executed concurrently while previous instances were still in progress, causing excessive JobRunner resource utilization.
- (HUB-48465). Fixed an issue where vulnerability remediation updates and status changes were not recorded in the project version activity journal.

- (HUB-48466). Fixed an issue where searching for components in use (`/api/search/components-in-use`) using quoted strings did not prioritize exact matches at the top of the search results.
- (HUB-48515). Fixed an issue where the Affected Projects list incorrectly displayed container layer components that had been removed or replaced.
- (HUB-48586). Fixed an issue where Black Duck SCA scans intermittently failed during BOM preparation with an unexpected `NOT_INCLUDED` scan status.
- (HUB-48614). Fixed an issue where uploading CycloneDX SBOM files containing certain Package URLs (such as Go pseudo-versions or special characters) failed with error `ERR05_1022 Unable to process SBOM matching request`.
- (HUB-48617). Fixed an issue where exported CycloneDX SBOM reports contained mismatched vulnerability scores and identifiers compared to what was displayed on the UI BOM.
- (HUB-48689). Fixed a regression where querying the `/vulnerable-bom-components` endpoint with `filter=ignored:true` failed to return components marked with component-level ignores.
- (HUB-48696). Fixed an issue where Black Duck Detect scans utilizing the `detect.project.user.groups` parameter failed if the scanning user lacked global administrative permissions.
- (HUB-48709). Fixed an issue where searching projects via `/api/projects?q=name:<project>` returned duplicate project records when a user held access through both direct assignment and project group memberships.
- (HUB-48752). Fixed an issue where policy rules evaluating the condition *Unconfirmed Snippets equals Yes* were erroneously triggered by ignored snippet matches.
- (HUB-48767). Fixed an issue where exported CycloneDX 1.6 and SPDX 3.0 SBOM reports omitted associated BDSA entries and populated unassociated CVE records instead.
- (HUB-48842). Fixed an issue where binary scans intermittently failed with `ERR05_1079 Internal Server Error` due to a transient 403 response during SCASS status polling.
- (HUB-48857). Fixed an issue where generated SBOM reports included vulnerability entries referencing components and versions that were not part of the project's BOM.
- (HUB-48896). Fixed a UI regression in Snippet View where candidate match details in the **Alternative Matches** dropdown were misaligned and truncated.
- (HUB-49090). Fixed an issue where users assigned direct access to a project could not be designated as the project owner.

Black Duck SCA 2026.7.0

Announcements

Upcoming removal of the Archived project version phase

The Archived project version phase will be removed in a future release (2026.11.0). Starting with that release, all capabilities related to the Archived project phase will no longer be available.

If you have project versions currently in the archived phase, we strongly recommend transitioning them to LTS before upgrading. Any Archived project versions remaining at the time of upgrade will be automatically transitioned to LTS.

Upcoming upgrade restrictions for PostgreSQL container users

In the upcoming 2026.10.0 release, users of the Black Duck SCA-supplied PostgreSQL container should be aware of new upgrade restrictions. This version will only support direct upgrades from Black Duck SCA versions that utilize PostgreSQL 15 or PG 16 containers, specifically covering all Black Duck SCA versions between 2024.10.0 and 2026.7.x (inclusive).

For users upgrading from older Black Duck SCA versions (prior to 2024.10.0), a two-step upgrade process will be required: first, upgrade to version 2025.7.x (or later), and then proceed to upgrade to version 2026.10.x.

Upcoming PostgreSQL container migration to version 17

Starting in **2026.10.0**, Black Duck SCA will upgrade the PostgreSQL container image to PostgreSQL 17. This migration ensures improved performance, stability, and access to the latest PostgreSQL features. Customers using the packaged PostgreSQL container should validate their environments for compatibility with PostgreSQL 17 prior to upgrading. No action is required for those using external databases.

Upcoming end of support for PostgreSQL 16

Support for **PostgreSQL 16** will end with the **2026.10.0** release of Black Duck SCA.

Users currently using the PostgreSQL 16 container should plan to upgrade to PostgreSQL 17 by of before that release.

External database configurations should follow standard compatibility guidance.

PostgreSQL 18 support for external databases

Black Duck SCA now supports and recommends PostgreSQL 18 for new installs that use external PostgreSQL.

Migrating to 2026.7.x does not require migration to PostgreSQL 18.

No action is required for users of the internal PostgreSQL container.

New and Changed Features

Black Duck SCA MCP Server

Black Duck now includes an MCP (Model Context Protocol) server that connects AI coding assistants directly to your Black Duck SCA instance. This enables developers to investigate security posture, triage vulnerabilities, generate compliance reports, and run scans — all from within their IDE or AI assistant.

Supported capabilities:

- **SBOM, VEX, and Notices report generation** — Generate SBOMs (with template selection), VEX reports, and basic notices reports for scanned projects.
- **Vulnerability triage and remediation** — Ignore or triage CVEs/BDSAs, and upgrade vulnerable components directly using the project-version-level API.
- **Policy violation summary** — Retrieve and review policy violations with remediation suggestions based on criticality.
- **Project and version search** — Search for existing projects using package manager or git metadata.
- **Source, binary, container, and SBOM scanning** — Run scans, check scan status, and match code snippets.

- **Dashboard summary** — View instance-wide security posture, activity trends, and vulnerability breakdowns.

For full installation, configuration, and troubleshooting details, see the Black Duck SCA MCP Server documentation.

Custom component vulnerability association Using CPEs

Custom component versions can now be associated with vulnerabilities using Common Platform Enumeration (CPE) identifiers. When a valid CPE 2.3 value is assigned to a custom component version, Black Duck SCA displays associated vulnerabilities on a dedicated Vulnerabilities tab and includes them in BOM risk calculations, policy evaluation, notifications, and reports. This helps organizations better manage vulnerability risk for commercial, proprietary, internal, or otherwise non-KnowledgeBase components.

VEX export templates

Create and manage VEX templates to control the content of CSAF 2.0 (VEX) reports. Templates are configured under the renamed **SBOM and VEX Templates** page (Manage > SBOM and VEX Templates), which now contains separate tabs for SBOM and VEX templates.

What's new:

- Reusable VEX templates with configurable fields: Legal Disclaimer, TLP Designation, Subprojects Vulnerabilities, Comments, and Vulnerability Type (CVE, BDSA, EUVD)
- VEX Template dropdown added to the report generation dialog
- Pre-configured System template included out of the box
- VEX Templates tab visible when the VEX module is enabled in your license

KnowledgeBase support bundle generation

You can now generate a KnowledgeBase (KB) support bundle directly from the BOM and the Match Review page. When you encounter discrepancies in component identification, licensing, or vulnerability data, select one or more components and choose **Generate Support Bundle**. The bundle collects all relevant component data — including match details, license information, vulnerability data, and optionally BDIO files — into a downloadable `.zip` file that you can attach to a support case. This eliminates the manual back-and-forth of gathering diagnostic information and helps the support team investigate issues more efficiently.

EUVD vulnerability identifiers now included in SBOM reports

SBOM reports now include EUVD (European Vulnerability Database) identifiers alongside CVE and BDSA identifiers, supporting Cyber Resilience Act (CRA) compliance requirements. EUVD data appears in CycloneDX (all versions) and SPDX 3.0 reports.

Existing SBOM export templates will have EUVD enabled automatically after upgrading to 2026.7.0.

SPDX 2.x reports are not affected by this change.

Configurable retention for New Vulnerabilities data

Administrators can now configure retention for **New Vulnerabilities** data. The new option in **Admin > System Settings > Data Retention** allows you to specify a retention period of **7 to 30 days**, with a default of **10 days**.

The configured retention period also determines the amount of historical data available through the date range filter on the **New Vulnerabilities** dashboard.

Vulnerability sub-status support in policy rules

You can now create more granular policy rules using vulnerability sub-statuses. When configuring a Vulnerability Condition with a Remediation Status of **Known Affected** or **Known Not Affected**, you can optionally specify a sub-status to narrow the policy evaluation.

Available sub-statuses for Known Affected: Mitigation, No Fix Planned, None Available, Vendor Fix, Workaround.

Available sub-statuses for Known Not Affected: Component Not Present, Vulnerable Code Not Present, Vulnerable Code Cannot be Controlled by Adversary, Vulnerable Code Not in Execute Path, Inline Mitigations Already Exist.

If no sub-status is selected, the policy evaluates against the status alone (matching existing behavior). Existing policy rules are unaffected by this change.

AI-assisted documentation search

Black Duck SCA 2026.7.0 introduces an AI-assisted documentation search experience that helps users quickly find relevant documentation directly from within the application.

- Access AI-assisted documentation search from the Help menu without leaving Black Duck SCA.
- Improve documentation discovery with AI-powered search capabilities designed to return more relevant results.
- System Administrators can enable or disable the AI-Assisted Documentation Service from **Admin** → **System Settings** → **System** → **Help**. The service is enabled by default.
- When enabled, documentation search requests are processed by an external cloud-based service to provide AI-assisted search functionality. Organizations that do not want documentation search requests processed externally can disable the service and continue using the legacy documentation experience.
- Air-gapped deployments continue to use the legacy documentation experience and are not affected by this feature.

Centralized component catalog (Phase 1)

Black Duck SCA 2026.7.0 introduces a centralized component catalog that normalizes component, component version, component origin, and vulnerability data into shared local database tables. This architectural improvement reduces the number of API requests made to KnowledgeBase services during BOM computation and KB update processing.

Customers can expect:

- **Faster BOM computation** — Component and vulnerability data is now cached locally, reducing round trips to the KnowledgeBase. Since most scans are rescans, the required data will typically already be present in the local catalog.
- **More reliable scan processing** — Fewer external KB API calls during BOM computation means fewer scan failures caused by KB connectivity or availability issues.
- **Faster and more reliable KB updates** — Data normalization allows the KB update job to process component and vulnerability updates more efficiently.
- **Reduced network egress** — Individual Black Duck SCA deployments will make fewer API requests to KB API services for components, versions, origins, and mapped vulnerabilities, reducing network egress costs.

There are no changes to the user interface, public APIs, or existing workflows. All BOM computation results, component data, vulnerability data, policy evaluations, and SBOM exports remain functionally identical.

Note: The database migration that runs during the upgrade to 2026.7.0 moves component data into centralized catalog tables. Depending on the size of your database, this migration may extend the upgrade window. Plan accordingly.

Updated BDSA auto-remediation behavior

BDSA auto-remediation no longer supports “apply” functionality. End-users may still enable or disable BDSA auto-remediation but it will only apply for following scans and changes.

Minimum supported browser versions

- Safari Version 17.6
- Chrome Version 127 (x86_64)
- Firefox Version 128 (64-bit)
- Microsoft Edge Version 127 (64-bit)

Container versions

- blackducksoftware/blackduck-postgres:16-2.9
- blackducksoftware/blackduck-postgres-upgrader:16-1.4
- blackducksoftware/blackduck-postgres-waiter:1.0.21
- blackducksoftware/blackduck-cfssl:1.0.38
- blackducksoftware/blackduck-nginx:2026.7.0
- blackducksoftware/blackduck-logstash:1.0.47
- blackducksoftware/bdba-worker:2026.6.1
- blackducksoftware/rabbitmq:1.2.50
- blackducksoftware/blackduck-authentication:2026.7.0
- blackducksoftware/blackduck-bomengine:2026.7.0
- blackducksoftware/blackduck-documentation:2026.7.0
- blackducksoftware/blackduck-integration:2026.7.0
- blackducksoftware/blackduck-jobrunner:2026.7.0
- blackducksoftware/blackduck-redis:2026.7.0
- blackducksoftware/blackduck-registration:2026.7.0
- blackducksoftware/blackduck-scanmatch:2026.7.0
- blackducksoftware/blackduck-storage:2026.7.0
- blackducksoftware/blackduck-webapp:2026.7.0

API Enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck SCA.

Removal of User Token API

As previously announced in the 2026.1.0 release, the following API related to user tokens has been removed in this update. Any requests to this API will now result in an HTTP 410 Gone response, indicating that the resource is no longer available:

- `PUT /api/current-user/tokens/<token-id>`

Sunset of Component Vulnerability APIs

As part of our ongoing efforts to streamline our API offerings, the component vulnerability APIs (`/api/components/<component-id>/vulnerabilities`) have undergone several changes in recent releases. These APIs were first deprecated, then reduced in functionality, and subsequently adjusted to return an HTTP 410 Gone response.

With this release, we are completing the sunset process by removing the component vulnerability APIs entirely. Users are encouraged to transition to alternative solutions as needed.

Binary Scanner Information

The binary scanner has been updated to version **2026.6.1**.

Fixed Issues

The following customer-reported issues have been fixed in this release:

- (HUB-45901). Fixed an issue where BDBA integrated scanning of ISO files produced significantly more unmatched components compared to BDBA standalone results. The scanner was not correctly detecting the Linux distribution namespace for RPM packages, which prevented components from being matched in the Knowledge Base.
- (HUB-46960). Fixed an issue where the Results Summary Graph percentages did not add up to 100% when using Saved Searches. The "Unknown" risk category was not being included in the percentage calculation.
- (HUB-47100). Fixed an issue where a project version could become permanently stuck in "converting to LTS" mode, preventing rescans and blocking deletion via the API.
- (HUB-47372). Added Match Review APIs (filtering, reviewing, ignoring, editing, and bulk actions for unmatched components) to the public API documentation.
- (HUB-47731). Fixed a NullPointerException in the RunAsService that occurred when the registration ID was temporarily unavailable, causing KB vulnerability lookups to fail.
- (HUB-47732). Fixed a recurring JobPersistenceException in the Quartz scheduler's misfire handler caused by missing trigger records, which affected scheduled job recovery across many deployments.
- (HUB-47748). Fixed an issue where vulnerability counts displayed in the summary boxes (Critical, High, Medium, Low) on the Component Version Overview page did not match the actual number of vulnerabilities listed in the table.
- (HUB-47787). Improved performance of the project search API, which previously executed a complex authorization query that consumed excessive database resources.
- (HUB-47911). Fixed an intermittent 500 error when updating file adjustments in the BOM editor, caused by a temporary table conflict.
- (HUB-47932). Corrected the LDAP configuration form so that the "Test Connection" button uses an updated Manager password without requiring a save first.

- (HUB-48227). Fixed an issue where selecting a file checkbox on the Snippet Adjustments Unconfirmed view also toggled an unrelated file. This occurred in project versions with multiple scans, where duplicate internal row identifiers caused checkbox state to be shared between different files.

Black Duck SCA 2026.4.x

Black Duck SCA 2026.4.2

Announcements

There are no announcements for Black Duck SCA 2026.4.2.

New and Changed Features

There are no changes in Black Duck SCA 2026.4.2.

Container versions

- blackducksoftware/blackduck-postgres:16-2.8
- blackducksoftware/blackduck-postgres-upgrader:16-1.4
- blackducksoftware/blackduck-postgres-waiter:1.0.20
- blackducksoftware/blackduck-cfssl:1.0.37
- blackducksoftware/blackduck-nginx:2026.4.2
- blackducksoftware/blackduck-logstash:1.0.45
- blackducksoftware/bdba-worker:2026.3.1
- blackducksoftware/rabbitmq:1.2.49
- blackducksoftware/blackduck-authentication:2026.4.2
- blackducksoftware/blackduck-bomengine:2026.4.2
- blackducksoftware/blackduck-documentation:2026.4.2
- blackducksoftware/blackduck-integration:2026.4.2
- blackducksoftware/blackduck-jobrunner:2026.4.2
- blackducksoftware/blackduck-redis:2026.4.2
- blackducksoftware/blackduck-registration:2026.4.2
- blackducksoftware/blackduck-scanmatch:2026.4.2
- blackducksoftware/blackduck-storage:2026.4.2
- blackducksoftware/blackduck-webapp:2026.4.2

API Enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck SCA.

There are no changes in Black Duck SCA 2026.4.2.

Binary Scanner Information

The binary scanner has been updated to version **2026.3.1**.

Fixed Issues

The following customer-reported issues have been fixed in this release:

- (HUB-47911). Fixed an issue where BOM file adjustments would intermittently fail with an "Unknown error" when editing matches on project versions with multiple contributing code locations. This was due to a temporary database table being created multiple times within a single transaction.

Black Duck SCA 2026.4.1

Announcements

There are no announcements for Black Duck SCA 2026.4.1

New and Changed Features

Registration page buttons disabled for airgapped installations

The **Refresh** and **Reset** buttons on the Product Registration page are now disabled for air-gapped (offline) deployments of Black Duck SCA when the air-gapped environment variable is enabled in the orchestration configuration. Previously, using these buttons in an air-gapped environment could leave the registration in an unrecoverable state, as the activation request cannot reach the external registration server. These buttons are now automatically hidden when the air-gapped flag is present, preventing potential registration issues.

Include Subproject Vulnerabilities in VEX Reports

VEX CSAF 2.0 reports now support the inclusion of vulnerability data from sub-projects. A new **Include Subproject Vulnerabilities** checkbox is available in the report creation dialog when generating a VEX report from either the global Reports page or a specific project version. When enabled, Black Duck SCA recursively discovers all sub-projects within the selected project's hierarchy and merges their vulnerability data into the report.

Container versions

- blackducksoftware/blackduck-postgres:16-2.8
- blackducksoftware/blackduck-postgres-upgrader:16-1.4
- blackducksoftware/blackduck-postgres-waiter:1.0.20
- blackducksoftware/blackduck-cfssl:1.0.37
- blackducksoftware/blackduck-nginx:2026.4.1
- blackducksoftware/blackduck-logstash:1.0.45
- blackducksoftware/bdba-worker:2026.3.1
- blackducksoftware/rabbitmq:1.2.49
- blackducksoftware/blackduck-authentication:2026.4.1
- blackducksoftware/blackduck-bomengine:2026.4.1
- blackducksoftware/blackduck-documentation:2026.4.1

- blackducksoftware/blackduck-integration:2026.4.1
- blackducksoftware/blackduck-jobrunner:2026.4.1
- blackducksoftware/blackduck-redis:2026.4.1
- blackducksoftware/blackduck-registration:2026.4.1
- blackducksoftware/blackduck-scanmatch:2026.4.1
- blackducksoftware/blackduck-storage:2026.4.1
- blackducksoftware/blackduck-webapp:2026.4.1

API Enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck SCA.

There are no changes in Black Duck SCA 2026.4.1

Binary Scanner Information

The binary scanner has been updated to version **2026.3.1**.

Fixed Issues

The following customer-reported issues have been fixed in this release:

- (HUB-46114). Resolved an issue where bulk editing the Usage field on SBOM-imported component matches appeared to succeed but did not save the updated value. Bulk usage changes on SBOM-imported matches are now saved correctly.
- (HUB-46529). Resolved a security issue where users with the **Project Creator** role could retrieve sensitive user metadata via the REST API, despite the UI correctly restricting this access. Access controls have been updated to align API behavior with the UI, preventing non-admin users from accessing user management data.
- (HUB-46628). Resolved an issue where subprojects added to the BOM defaulted to an "Unreviewed" approval status with no way to change it, resulting in unavoidable policy violations. A new Approval Status field has been added at the Project Version level in Settings, allowing users to set the review status for subproject versions. This field is also supported via bulk actions in the Components tab and is carried over when cloning a project version.
- (HUB-47787). Resolved a performance issue with the `GET /api/projects` API where unnecessary database operations were causing slower response times. This optimization reduces query complexity and improves overall API performance, particularly for large deployments.
- (HUB-47826). Fixed an issue where the "SBOM" match type was missing from the Component Match Type table in the Reporting Database documentation.
- (HUB-47843). Fixed an issue where SBOM report generation failed with a NullPointerException when the report included subproject components.

Black Duck SCA 2026.4.0

Announcements

End of Support for BD SCA Embedded Web Help

We are announcing the upcoming end of support for the Black Duck SCA embedded web help with Black Duck SCA 2026.7.0. As part of this transition, documentation will be moving to a new URL and IP address.

For customers using air-gapped Knowledge Bases, a PDF help document will be provided going forward as an alternative resource.

Please note that the documentation container will reach its end of life, and we encourage all users to prepare for this change.

Chainguard Container Image Support

Black Duck SCA Secure Container now supports Chainguard container images, helping organizations that rely on commercially maintained containers reduce risk, eliminate noise, and move faster. By combining Chainguard's curated component inventory and vulnerability intelligence with Black Duck SCA's industry#leading analysis, customers get more accurate results with fewer false positives, faster access to security fixes, and less manual triage for developers and security teams. The result is quicker patching, lower exposure to vulnerabilities, and more time spent delivering secure software instead of tracking down issues.

Preliminary PostgreSQL 18 support

Black Duck SCA 2026.4.0 introduces preliminary support for PostgreSQL 18 as an external database. This support is for **testing purposes only**, and **production use is not supported** at this time. Customers can evaluate PostgreSQL 18 in non-production environments to assess compatibility ahead of future full support.

NOTE: Starting with PostgreSQL 18, data page checksums are enabled by default when initializing a new cluster. If you are upgrading from a previous PostgreSQL version using `pg_upgrade`, you'll need to add the `--no-data-checksums` option to `initdb` when initializing the PostgreSQL 18 cluster.

Retroactive PostgreSQL 17 support

With the release of Black Duck SCA 2026.4.0, we are pleased to announce retroactive support for PostgreSQL 17 as an external database. This support is intended for production use, allowing customers to leverage PostgreSQL 17 in their environments. Customers are encouraged to upgrade to PostgreSQL 17 to benefit from the latest features and enhancements.

Update to `default_statistics_target` Setting in Black Duck SCA 2026.4.0

With the migration to Black Duck SCA 2026.4.0, the `default_statistics_target` setting for PostgreSQL will be increased to 250, provided that it is not already set to a higher value.

Important Considerations:

- For users utilizing external PostgreSQL instances, the change may fail to apply if the `bds_hub` database is not owned by the `blackduck` database user or if the `blackduck` user lacks administrative privileges. Should this failure occur, it will not impede the migration process and may go unnoticed by the user.
- Users operating with the Black Duck-provided PostgreSQL container are not affected by these conditions, and no additional action is required.

Verification Steps for External PostgreSQL Users: To confirm whether the new value has been successfully applied, connect to the `bds_hub` database and execute the following command:

```
SHOW default_statistics_target;
```

If the returned value is below 250, it can be updated using the following command:

```
ALTER DATABASE bds_hub SET default_statistics_target = 250;
```

Please note that the migration process sets this value specifically for the `bds_hub` database. As a result, queries checking the system-wide setting may not reflect this change, even if the update was successfully applied for `bds_hub`.

New and Changed Features

Integration of EUVD Vulnerability Data into VEX Reports

As part of compliance with the NIS2 directive, we are introducing support for European vulnerability data from the European Vulnerability Database (EUVD) in VEX (Vulnerability Exploitability eXchange) reports. This enhancement aligns with efforts to improve coordinated vulnerability reporting under NIS2 and the Cyber Resilience Act (CRA).

Key Features:

- **EUVD Reference Integration:** Vulnerability data published from the EUVD will be included as related reference IDs in our BDSA and CVE VEX reporting processes. Note that EUVD vulnerabilities will not be directly ingested as a separate type of vulnerability.
- **Link to EUVD Records:** Each EUVD record will be linked in the vulnerability description field on the Vulnerabilities tab, mirroring the link to the external EUVD site found in the corresponding CVE record. A warning will be displayed about navigating to an external site.
- **API Support:** APIs are available to obtain additional EUVD details.
- **CSAF 2.0 VEX Report Enhancements:** The EUVD ID and description will be included as additional identifiers in the existing vulnerability entries in the vulnerabilities/id and vulnerabilities/id/description fields of the CSAF 2.0 VEX report.
- **System Setting for VEX Reports:** A system setting will allow toggling the exclusion of BDSA IDs in VEX reports, located under Administration > System Settings > SBOM. The toggle's default value will be "Off."

Introduction of TLP Designation for VEX Documents

Black Duck SCA 2026.4.0 introduces the Traffic Light Protocol (TLP) designation feature for VEX (Vulnerability Exploitability eXchange) documents. This enhancement allows users to specify the appropriate TLP label for information sharing, ensuring clarity on how the information should be treated by recipients.

Users can select the appropriate TLP designation from a dropdown menu within the project-level SBOM fields. The selected TLP value will be included in the VEX document, adhering to the format defined by FIRST.org.

Enhanced SBOM PURL Field for Component Versions

The SBOM PURL field for component versions has been updated to display all matching origin IDs when multiple PURL matches are available. Users will see a notification indicating the number of PURL matches for a component version, allowing for better visibility and selection options. When there are multiple PURL

matches, users can choose one of the displayed matches or enter their own custom PURL to override the default selection. Each selected PURL will be included in the SBOM report.

Central Configuration for Correlated Scanning

To streamline the enablement of correlated scanning for all customers, Black Duck SCA 2026.4.0 introduces a new global configuration option for the Detect parameter `detect.blackduck.correlated.scanning.enabled`.

To take advantage of this feature, you must have Detect 11.4.0+ and SCASS must be enabled on your product registration key.

Correlated Scanning can be enabled from **Admin → System Settings → Black Duck Detect**.

Option to Globally Disable Automatic Unmapping for SBOM Import Scan Types

Black Duck SCA now includes an option to globally disable the automatic unmapping of scan types for SBOM (Software Bill of Materials) imports.

This enhancement prevents unintended unmapping of SBOMs when multiple SBOMs are imported into the same project version. By excluding SBOM scan types from the automatic unmapping functionality, users can maintain their manual mappings, ensuring greater accuracy and control over the mapping process.

Enhanced Data Table and Dashboard Row Selection

The user interface has been updated to allow users to select the number of rows displayed per page in data tables and dashboards throughout the application. Users can now choose from page size options of 25, 50, 100, 250, and 500 items per page. Please be aware that selecting larger page sizes may result in slower loading times, as the backend processes a greater number of rows.

Deprecation of Detect 9 in Detect Version Management

With the release of Detect 11 on October 30, 2025, and the end of service for Detect 9.x scheduled for April 2026, Black Duck SCA has deprecated support for Detect 9 in the Detect Version Management page.

For customers upgrading with Detect 9.x already selected, a red warning indicator and message will appear, advising that Detect 9 has reached end of support and recommending an upgrade. Additionally, users will be warned that switching the central configuration away from Detect 9.x is irreversible. Detect 9.x will no longer appear as an option for fresh installs, remaining visible only for customers who had it selected prior to upgrading. Furthermore, Detect 11 will be set as the default version for new customers or upgrades to version 2026.4.0 where the detect version property was previously null.

Removal of Multi-Project Option from Global CSAF VEX Report

The Multi-Project option has been removed from the Global CSAF VEX report. This decision was made to simplify the management of document-level attributes, as the use case for including multiple projects in a single VEX document is deemed unlikely.

Key Changes:

- The project selection in the Global CSAF VEX report has been modified to a single selection dropdown, allowing users to type and filter project names. The multi-select feature is no longer available, and reports can only be generated for a single project.
- The API supporting multiple projects in a single VEX report has been deprecated. Users will receive a warning when using the old endpoint, indicating that they may encounter unexpected results regarding document-level data.

Removal of Datadog from Helm Charts

Datadog has been discontinued, and as a result, all references to Datadog will be removed from the Helm Charts. With the removal of Datadog from our Helm Charts, customers are encouraged to review their current monitoring setups and explore alternative solutions to ensure your monitoring needs are met.

Added Support for Docker versions 29.x & 28.x

Black Duck SCA has aded support for the latest Docker versions 29.x and 28.x. This enhancement ensures compatibility with the newest features and improvements in Docker, allowing users to effectively manage and secure their containerized applications. Customers are encouraged to update to these versions to take advantage of the latest capabilities in Black Duck SCA.

Minimum supported browser versions

- Safari Version 17.4
- Chrome Version 124 (x86_64)
- Firefox Version 125 (64-bit)
- Microsoft Edge Version 124 (64-bit)

Container versions

- blackducksoftware/blackduck-postgres:16-2.7
- blackducksoftware/blackduck-postgres-upgrader:16-1.3
- blackducksoftware/blackduck-postgres-waiter:1.0.20
- blackducksoftware/blackduck-cfssl:1.0.36
- blackducksoftware/blackduck-nginx:2026.4.0
- blackducksoftware/blackduck-logstash:1.0.45
- blackducksoftware/bdba-worker:2026.3.1
- blackducksoftware/rabbitmq:1.2.49
- blackducksoftware/blackduck-authentication:2026.4.0
- blackducksoftware/blackduck-bomengine:2026.4.0
- blackducksoftware/blackduck-documentation:2026.4.0
- blackducksoftware/blackduck-integration:2026.4.0
- blackducksoftware/blackduck-jobrunner:2026.4.0
- blackducksoftware/blackduck-redis:2026.4.0
- blackducksoftware/blackduck-registration:2026.4.0
- blackducksoftware/blackduck-scanmatch:2026.4.0
- blackducksoftware/blackduck-storage:2026.4.0
- blackducksoftware/blackduck-webapp:2026.4.0

API Enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck SCA.

New endpoints to support setting Detect parameters

The following API endpoints have been added to support setting Detect parameters in Black Duck SCA.

- `PATCH api/settings/detect/properties`
- `GET api/settings/detect/properties`

Removal of [PUT] /api/current-user/tokens/<token-id> links

The `PUT /api/current-user/tokens/<token-id>` endpoint was marked for deprecation starting in Black Duck SCA 2026.1.0. In Black Duck SCA 2026.4.0, all meta link references to this deprecated endpoint has been removed.

Binary Scanner Information

The binary scanner has been updated to version **2026.3.1**.

Fixed Issues

The following customer-reported issues have been fixed in this release:

- (HUB-40429). Resolved an issue where the Black Duck binary scan failed to identify the Qt version 5.15.12. The scanner successfully detected the version in the BDIO export; however, it was not mapped to the correct channel, leading to identification issues.
- (HUB-46005). Resolved discrepancies in security risk counts following the upgrade to version 2025.4.2, where risk profiles were not updating correctly despite synchronized vulnerability counts.
- (HUB-46626). Investigated and addressed an issue where file paths were displayed as URL-encoded strings in the side-by-side snippet view.
- (HUB-46899). Resolved a bug affecting vulnerability prioritization where selecting NVD in Security Risk Ranking incorrectly displayed BDSA entries. The issue stemmed from a bug in the security re-ranking code, linked to changes in how vulnerability summaries are stored and processed following a recent update.
- (HUB-46929). Fixed an issue where custom component matches were ignored during the matching process when SCASS (cloud-based matching) was enabled, causing all custom-mapped origins to remain unmatched.
- (HUB-46968). Fixed a regression in version 2025.10.1 where converting a project version to LTS with the CycloneDX v1.6 specification incorrectly produced SPDX format reports.
- (HUB-46991). Fixed a bug in Black Duck SCA where scan sizes between 1,000 and 1,024 MB were incorrectly displayed as “KMB.”
- (HUB-47062). Resolved an issue where discrepancies between the notification workflow, activity logs, and database records were causing notifications for new vulnerabilities to go missing after KB updates in project versions.
- (HUB-47311). Resolved an issue with a security feature that incorrectly blocked the /api/search/components-in-use endpoint, resulting in 400 errors during normal usage.

Black Duck SCA 2026.1.x

Black Duck SCA 2026.1.2

Announcements

There are no announcements for 2026.1.2.

New and Changed Features

There are no new or changed features in Black Duck SCA 2026.1.2.

Container versions

- blackducksoftware/blackduck-postgres:16-2.7
- blackducksoftware/blackduck-postgres-upgrader:16-1.3
- blackducksoftware/blackduck-postgres-waiter:1.0.19
- blackducksoftware/blackduck-cfssl:1.0.35
- blackducksoftware/blackduck-nginx:2026.1.2
- blackducksoftware/blackduck-logstash:1.0.45
- blackducksoftware/bdba-worker:2025.12.5
- blackducksoftware/rabbitmq:1.2.49
- blackducksoftware/blackduck-authentication:2026.1.2
- blackducksoftware/blackduck-bomengine:2026.1.2
- blackducksoftware/blackduck-documentation:2026.1.2
- blackducksoftware/blackduck-integration:2026.1.2
- blackducksoftware/blackduck-jobrunner:2026.1.2
- blackducksoftware/blackduck-redis:2026.1.2
- blackducksoftware/blackduck-registration:2026.1.2
- blackducksoftware/blackduck-scanmatch:2026.1.2
- blackducksoftware/blackduck-storage:2026.1.2
- blackducksoftware/blackduck-webapp:2026.1.2

API Enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck SCA.

There are no changes in 2026.1.2.

Binary Scanner Information

The binary scanner has been updated to version **2025.12.5**.

Fixed Issues

The following issues have been fixed in this release:

- (HUB-47787). Fixed an issue where the project search API (`GET /api/projects`) caused excessive database resource consumption due to an inefficient authorization query. The query unnecessarily joined `central_project_version` and `version_bom` tables when resolving project access, resulting in degraded database performance under load. The authorization query has been optimized to remove these unnecessary joins, significantly reducing database utilization.
- (HUB-47791). Fixed a performance issue where high-volume read queries on the component_adjustment table executed full sequential scans, resulting in significantly degraded performance on deployments with large BOM datasets. Database indexes have been added on the `project_id` and `version_id` columns to ensure efficient query execution.

Black Duck SCA 2026.1.1

Announcements

There are no announcements for 2026.1.1.

New and Changed Features

VEX Product ID and Filename Configuration

VEX reports now support configurable Product IDs and filenames to align with the CSAF 2.0 VEX specification. A VEX Product ID can be defined at the project level and is used to populate both the VEX report filename and the document > tracking > ID field in generated VEX reports.

- For single project version reports, the VEX Product ID is combined with the project version to form the filename and tracking ID
- For single project Global reports, the VEX Product ID is used as-is without appending the project version
- For multi-project Global reports, existing logic is used regardless of VEX Product ID configuration (multi-project support coming in a future release)

The VEX Product ID must be unique within a single Black Duck SCA instance. Uniqueness across multiple instances cannot be guaranteed or enforced.

Note: Available only for customers with Vulnerability Exploitability eXchange (VEX) enabled on their product registration.

VEX Legal Disclaimer

VEX reports now support automatic inclusion of organization-level legal disclaimers. Configure your legal disclaimer at the organization or project group level to define terms and conditions for VEX document access. The disclaimer is automatically included in all VEX reports when populated and cannot be excluded.

Note: Available only for customers with Vulnerability Exploitability eXchange (VEX) enabled on their product registration.

Updated Status Mappings

Updated Black Duck SCA vulnerability status mappings for CSAF VEX reports:

- `NEW` status is now included in VEX reports and maps to `under_investigation`
- `MITIGATED` status now maps to `known_not_affected` with justification `inline_mitigations_already_exist` (changed from `FIXED`)

Updated Black Duck SCA vulnerability status mappings for SPDX 3 reports:

- `NEW` status now maps to `underInvestigationFor`
- `MITIGATED` status now maps to `doesNotAffect` with justification `"security_justificationType": "inlineMitigationsAlreadyExist"`

Updated Black Duck SCA vulnerability status mappings for CycloneDX reports:

- `NEW` status now maps to `in_triage`
- `MITIGATED` status now maps to `not_affected` with justification `protected_by_mitigating_control`

Deprecation Notice: BDSA Auto Remediation Apply Functionality

The ability to immediately **Apply** BDSA Auto Remediation configuration changes is deprecated and will be removed in release **2026.7.0**.

BDSA Auto Remediation configuration remains available, allowing administrators to enable or disable the feature. However, going forward, auto remediation will only apply to new and updated data changes rather than immediately applying to all existing data when the configuration is changed.

Administrators should review and update any workflows that rely on this functionality prior to upgrading.

Container versions

- blackducksoftware/blackduck-postgres:16-2.7
- blackducksoftware/blackduck-postgres-upgrader:16-1.3
- blackducksoftware/blackduck-postgres-waiter:1.0.19
- blackducksoftware/blackduck-cfssl:1.0.35
- blackducksoftware/blackduck-nginx:2026.1.1
- blackducksoftware/blackduck-logstash:1.0.45
- blackducksoftware/bdba-worker:2025.12.5
- blackducksoftware/rabbitmq:1.2.49
- blackducksoftware/blackduck-authentication:2026.1.1
- blackducksoftware/blackduck-bomengine:2026.1.1
- blackducksoftware/blackduck-documentation:2026.1.1
- blackducksoftware/blackduck-integration:2026.1.1
- blackducksoftware/blackduck-jobrunner:2026.1.1
- blackducksoftware/blackduck-redis:2026.1.1
- blackducksoftware/blackduck-registration:2026.1.1
- blackducksoftware/blackduck-scanmatch:2026.1.1
- blackducksoftware/blackduck-storage:2026.1.1
- blackducksoftware/blackduck-webapp:2026.1.1

API Enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck SCA.

There are no changes in 2026.1.1.

Binary Scanner Information

The binary scanner has been updated to version **2025.12.5**.

Fixed Issues

The following issues have been fixed in this release:

- (HUB-46731). Improved the consistency of CPE (Common Platform Enumeration) selection in CycloneDX SBOM reports. When multiple CPEs are associated with a component, Black Duck SCA now selects the first CPE from an alphabetically sorted list, rather than a random selection.
- (HUB-46925). Resolved a critical bug causing upgrade failures during PostgreSQL migration when upgrading from version 2025.4.1 to 2025.10.1 in Helm/Kubernetes deployments. Fixed the migration script to correctly set recursive permissions on the certs and data directories, preventing permission errors that caused database startup failures and potential data corruption.
- (HUB-47003). Fixed SPDX import failures caused by underscores in repository names within download locations. Updated the SPDX Java model dependency to resolve the parsing issue.
- (HUB-47166). Resolved an issue where policy rules with multiple vulnerability conditions were not correctly evaluating the "Published Age" filter.
- (HUB-47174). Addressed an unspecified documentation gap regarding global roles in Black Duck SCA; users with roles such as Security Manager were previously unable to assign project-level roles due to a system setting that was not clearly documented, leading to confusion.The Role Matrix and supporting documentation has been updated to clarify this behavior.
- (HUB-47175). Fixed an issue where SPDX SBOM files containing certain license references (such as Artistic-dist and libpng-1.6.35) previously failed to import into Black Duck SCA due to the SPDX library's outdated vendored license list (version 3.26). The SPDX library has been updated to support license list version 3.27.0, resolving the parsing errors and allowing affected SPDX files to import successfully.
- (HUB-47226). Updated the documentation to clarify that policy rules based solely on vulnerability scores do not automatically exclude remediated vulnerabilities. To have violations clear upon remediation, policy rules must include remediation status conditions in addition to score-based criteria.
- (HUB-47282). Fixed an issue where ignored items could temporarily appear on the BOM Components tab after upgrading to a version with Match Review enabled; now ignored components and snippets are properly hidden from the BOM Components tab until the first BOM computation, while remaining visible in the Match Review tab.

Black Duck SCA 2026.1.0

Announcements

Introduction of Match Review Process

With the Black Duck SCA 2026.1.x release, we are excited to introduce the Match Review process. This new feature will add a Review tab to the Bill of Materials, where certain items identified during scanning will be placed for further evaluation.

After the upgrade, existing Project Versions' Bills of Materials will initially appear unchanged. However, you will gain access to additional information about unmatched items in the new Review tab. Upon rescanning a Project Version with the updated software, you may notice some matches moving from the Bill of Materials to the Review tab.

New Project Versions will immediately incorporate this feature, displaying relevant scan contents in the Review tab right away. For more details, please refer to the User Guide.

Deprecation of Archived Project Phase

Effective immediately, the Archived project phase has been deprecated in favor of Long Term Support (LTS) project versions.

With the introduction and ongoing enhancements to LTS project versions, we are transitioning away from the Archived phase to provide a more robust solution for managing released software artifacts that require ongoing vulnerability tracking and support:

- **No New Archived Versions**: New archived project versions can no longer be created.
- **Existing Archived Versions**: Current archived project versions will not be deleted or removed during upgrade. However, they will now be subject to data retention policies that will either transition them to LTS (by default) or delete them after the data retention period has been met (default 90 days).
- **Automated Transition**: An automated workflow will either delete existing archived project versions or transition them to LTS state, configurable through the System Administrator data retention settings page.
- **Mandatory Configuration**: This automated workflow cannot be disabled and must be configured by system administrators.
- **Future Removal**: The Archived project phase will be completely removed from Black Duck SCA in a future release.

Action Required: System administrators should review and configure the automated transition settings in the data retention settings page to ensure proper handling of existing archived project versions.

New and Changed Features

Preserve Component Relationships on SBOM Import

Black Duck SCA now preserves component relationships when importing SBOM reports, supporting compliance with CISA SBOM minimum requirements. This feature retains dependency information from SPDX v2 and v3 SBOMs, enabling accurate reproduction of relationships in exported reports and supporting enhanced vulnerability and license analysis.

New Footer Helper Bar

Black Duck SCA now includes a default footer helper bar that provides users with quick access to essential support resources. This enhancement improves user accessibility by offering convenient links to key services directly from the interface:

- **Community Portal**: Easy access to the Black Duck community for collaboration and knowledge sharing.
- **Share an Idea**: Quick link for users to submit feature requests and suggestions.

The footer is automatically added to new installations and upgrades that do not have existing footers, ensuring minimal disruption to current configurations.

Updated Functionality for Project Version Data Retention

In this release, we have enhanced the Project Version Auto-Deletion feature, now named Project Version Auto Actions, to provide users with greater control over managing project versions. Key updates include:

- **Automatic Progression to LTS**: Users can now configure project versions to automatically transition to Long-Term Support (LTS) status, ensuring that critical versions receive ongoing maintenance and security updates.
- **Updated UI**: The user interface has been updated to simplify the configuration process for these actions, making it more intuitive for users to set up automatic progression and deletion of project versions.

New Younger Than Operator for Components

A new date age operator, **"younger than,"** has been added to the **Component Release Age** and **Vulnerability Published Age** expression types. This operator allows users to identify components with release dates that are younger than a specified number of days (e.g., finding components released within the last 30 days):

- If a component is found to be in violation due to this operator, it will not automatically transition to **NOT_VIOLATION** status. The violation status will remain until a new scan or relevant BOM computation occurs.
- The minimum user value for this operator is set to 3 days, as rules to find components with release dates before now are not supported.

Updated Component Version Overview

We have made significant improvements to the Component Version Overview in the user interface. The layout has been updated to provide a more intuitive and streamlined experience.

- **New Layout:** The updated design enhances usability, making it easier to navigate and access important information about component versions.
- **Improved Information Display:** Key details are presented more clearly, allowing users to quickly find relevant data such as descriptions, known vulnerabilities, and associated licenses.
- **Enhanced User Experience:** The overall user experience has been improved, ensuring that users can efficiently manage and review component information.

Enhanced Bitbucket Data Center Onboarding

The user interface has been updated to allow for Bitbucket Data Center (BBDC) to onboard SCM projects in alignment with other workflows. This enhancement ensures that the existing workflow for BBDC now looks and operates similarly to other SCM options:

- Users can select one or multiple repositories for scanning on the same page.
- The scanning process will create a project for the selected repository.
- Users can delve into the project to find Bill of Materials (BOMs).
- The option to select other versions of the repository is now available, enabling users to initiate additional scans and retrieve BOMs.

This update streamlines the onboarding process for Bitbucket Data Center, providing a consistent experience across all SCM providers.

Support for Additional Image Formats in Logo Customization

We have enhanced the logo customization feature to support additional image formats. Users can now upload logos in various formats, including PNG, GIF, SVG, WEBP, JPEG, and AVIF.

Removal of Edit Feature for User Access Tokens

In this release, the edit feature for user access tokens has been removed. This change addresses security concerns associated with storing newly generated access tokens in plaintext, which can lead to poor security practices.

Access tokens are intended for single use upon generation, and users are encouraged to create new tokens as needed rather than copying and pasting existing ones. Inactive tokens will be purged, ensuring better management of access credentials.

Enhancement to External Link Confirmation UI Workflow

We have improved the external link confirmation workflow to enhance user experience. Previously, users were required to dismiss the confirmation popup every time they clicked an external link, even when the full URL was displayed.

Key Changes:

- The confirmation modal now appears only when the link text does not match the actual URL, ensuring transparency about the link's destination.
- The confirmation modal will close automatically after the user clicks "Confirm," streamlining the process.

Removal of SCASS Enablement Documentation

The documentation page describing how to manually enable SCASS has been removed. This information is now outdated, as customers can no longer enable SCASS themselves. SCASS enablement is now handled entirely through the customer’s registration key, and no configuration file changes are required. Customers who wish to enable SCASS or need guidance regarding their SCASS eligibility should contact Support for assistance.

Minimum supported browser versions

- Safari Version 17.1
- Chrome Version 119 (x86_64)
- Firefox Version 119 (64-bit)
- Microsoft Edge Version 119 (64-bit)

Container versions

- blackducksoftware/blackduck-postgres:16-2.6
- blackducksoftware/blackduck-postgres-upgrader:16-1.2
- blackducksoftware/blackduck-postgres-waiter:1.0.19
- blackducksoftware/blackduck-cfssl:1.0.35
- blackducksoftware/blackduck-nginx:2026.1.0
- blackducksoftware/blackduck-logstash:1.0.45
- blackducksoftware/bdba-worker:2025.12.1

- blackducksoftware/rabbitmq:1.2.49
- blackducksoftware/blackduck-authentication:2026.1.0
- blackducksoftware/blackduck-bomengine:2026.1.0
- blackducksoftware/blackduck-documentation:2026.1.0
- blackducksoftware/blackduck-integration:2026.1.0
- blackducksoftware/blackduck-jobrunner:2026.1.0
- blackducksoftware/blackduck-redis:2026.1.0
- blackducksoftware/blackduck-registration:2026.1.0
- blackducksoftware/blackduck-scanmatch:2026.1.0
- blackducksoftware/blackduck-storage:2026.1.0
- blackducksoftware/blackduck-webapp:2026.1.0

API Enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck SCA.

Update: Report Creation Endpoints

The following report creation endpoints now have the project version ID in the request payload changed from required to optional:

- `POST /api/versions/{projectVersionId}/reports`
- `POST /api/versions/{projectVersionId}/license-reports`
- `POST /api/projects/{projectId}/versions/{projectVersionId}/sbom-reports`
- `POST /api/lts-projects/{projectId}/lts-project-versions/{projectVersionId}/sbom-reports`

If the project version ID is provided in the request payload, it must match the project version ID specified in the API URI.

Deprecated Vulnerabilities API Removed

As a follow-up to the deprecation announced in 2025.10.0, the `GET /api/components/<component-id>/vulnerabilities` API endpoint has been modified in version 2026.1.0 to return `HTTP 410 Gone`.

Users are strongly encouraged to transition to the following API endpoints:

- `GET /api/components/<component-id>/versions/<version-id>/vulnerabilities`
- `GET /api/components/<component-id>/versions/<version-id>/origin/<origin-id>/vulnerabilities`

These endpoints provide more accurate and efficient access to vulnerability data for specific component versions and origins.

Deprecation and Removal of Data Retention APIs

The following changes have been made to the Data Retention API endpoints:

- `GET /api/settings/data-retention` (v4 and v5) — These endpoints have been **removed** and are no longer available.

- `PATCH /api/settings/data-retention` (v4 and v5) — These endpoints are now **deprecated** and will be removed in a future release.
- `GET /api/settings/data-retention` (v6) and `PATCH /api/settings/data-retention` (v6) — These endpoints remain **fully supported and available**.

These updates retire legacy versions of the Data Retention APIs and consolidate ongoing support into the v6 endpoints.

API Changes: ARCHIVED Phase No Longer Supported

The following APIs no longer accept the `ARCHIVED phase` as part of their requests:

- `POST /api/projects/{projectID}/versions`
- `PUT /api/projects/{projectID}/versions/{projectVersionID}`

Users who previously utilized the ARCHIVED phase in these endpoints will need to update their API calls accordingly. Please refer to the API documentation for current supported phases and recommended alternatives.

Deprecation of User Token API

The following API related to user tokens have been deprecated and will be removed in a future update. It will now return `HTTP 410 Gone`:

- `PUT /api/current-user/tokens/<token-id>`

Binary Scanner Information

The binary scanner has been updated to version **2025.12.1**.

Fixed Issues

The following customer-reported issues have been fixed in this release:

- (HUB-44108). Fixed excessive warning messages related to source VBC ID detection failures, specifically the message "Could not determine source VBC ID for child project when calculating license conflicts."
- (HUB-44352). Resolved a bug in the reporting database materialized view where reporting.component was counting/showing unconfirmed snippets in a project/version, causing discrepancies in BOM component counts.
- (HUB-45050). Resolved an SSL certificate mismatch issue during a Kubernetes upgrade that affected jobrunner health checks. The IPv4 address was added to the jobrunner's certificate SANs, eliminating SSLPeerUnverifiedException errors.
- (HUB-45320). Updated API Documentation to include the previously missing fields in the project representation for the projects API endpoint. The fields to be added are `deepLicenseDataEnabled`, `deepLicenseDataSnippetEnabled`, and `licenseConflictsEnabled`, which are returned in the response of the `GET /api/projects/{projectId}` endpoint.
- (HUB-45475). Resolved a bug that caused vulnerabilities to be omitted from the `components.csv` file after editing manual snippets with an origin set. Specifically, if components added as "Manually Identified, Snippet" were bulk edited using the 'Adjust Snippets and Confirm' option in the Source tab, their associated vulnerabilities were not included in the `components.csv` file. The fix ensures that vulnerabilities are correctly captured and reported in the file.
- (HUB-45694). Resolved the issue of missing supplier names in CycloneDX SBOM reports generated in Black Duck SCA.

- (HUB-45944). Resolved an issue where components present in an earlier (inner) layer of a container image but deleted in a higher (outer) layer were not recognized by the scanner as part of the final image. This issue resulted in components that had been removed still appearing in the Vulnerability Remediation Report during container scans.
- (HUB-46037). Addressed an issue where Nginx returned a 403 Forbidden response for requests to non-existent files (e.g., /metrics.json) instead of the expected 404 Not Found status.
- (HUB-46291). Resolved an issue where uploading a BDIO file exceeding the "Maximum code location size" silently failed without providing an error message to the user. Previously, users would see that the upload appeared successful, but the scan data would not be listed due to the failure occurring between upload and scan creation.
- (HUB-46359). Resolved a regression issue related to project settings that caused an invalid error message when setting unmatched file purging options.
- (HUB-46551). Fixed an issue where the License Terms page did not auto-refresh when activating or deactivating a license term.
- (HUB-46572). Resolved issue with remediation comments not showing in the UI after upgrading to version 2025.7.1. Previously, comments associated with components having a single origin were visible, but changes in functionality to display multiple origins for a component led to the disappearance of these comments in the UI.
- (HUB-46598). Resolved issues with large binary multi-part uploads in multi-node AKS deployments, which led to connection resets and message digest errors during re-assembly.
- (HUB-46642). Resolved issue where an inactive project group link was shown to a non-admin project group user.
- (HUB-46656). Improved performance of the `/api/projects` endpoint by optimizing view conversion in `ProjectV6ViewConverter` and reducing repetitive database queries, resulting in faster project listing and typeahead operations.
- (HUB-46669). Resolved a bug that caused an HTTP 400 Bad Request error when attempting to remove a hash from the Project Version SBOM fields.

Black Duck SCA 2025.10.x

Black Duck SCA 2025.10.2

Announcements

There are no new announcements for 2025.10.2.

New and Changed Features

Container versions

- blackducksoftware/blackduck-postgres:16-2.6
- blackducksoftware/blackduck-postgres-upgrader:16-1.2
- blackducksoftware/blackduck-postgres-waiter:1.0.18
- blackducksoftware/blackduck-cfssl:1.0.34
- blackducksoftware/blackduck-nginx:2025.10.2

- blackducksoftware/blackduck-logstash:1.0.45
- blackducksoftware/bdba-worker:2025.9.2
- blackducksoftware/rabbitmq:1.2.48
- blackducksoftware/blackduck-authentication:2025.10.2
- blackducksoftware/blackduck-bomengine:2025.10.2
- blackducksoftware/blackduck-documentation:2025.10.2
- blackducksoftware/blackduck-integration:2025.10.2
- blackducksoftware/blackduck-jobrunner:2025.10.2
- blackducksoftware/blackduck-redis:2025.10.2
- blackducksoftware/blackduck-registration:2025.10.2
- blackducksoftware/blackduck-scanmatch:2025.10.2
- blackducksoftware/blackduck-storage:2025.10.2
- blackducksoftware/blackduck-webapp:2025.10.2

API Enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

There are no new API enhancements in 2025.10.2.

Binary Scanner Information

The binary scanner has been updated to version **2025.9.2**.

Fixed Issues

The following issues have been fixed in this release:

- (HUB-46950). Fixed an issue where status was showing an error: Project name must be initialized.
- (HUB-47016). Fixed an issue where components with multiple licenses were incorrectly shown as “Unknown License” in Black Duck SCA.

Black Duck SCA 2025.10.1

Announcements

There are no new announcements for 2025.10.1.

New and Changed Features

Display of EUVD IDs in Vulnerability Records

We have enhanced the vulnerability record pages to include, if applicable, the ID of related vulnerabilities from the European Vulnerability Database (EUVD) in the page header. This improvement provides users with a more comprehensive view of related vulnerabilities, enhancing visibility and context for security management.

VEX Report Generation for Project Versions

Black Duck SCA now allows the generation of Vulnerability Exploitability EXchange (VEX) reports at the project version level. This enhancement enables users to assess vulnerabilities specific to each project version, facilitating targeted remediation efforts.

Users can create VEX reports detailing the status of vulnerabilities within individual project versions, improving decision-making and security management.

Container versions

- blackducksoftware/blackduck-postgres:16-2.5
- blackducksoftware/blackduck-postgres-upgrader:16-1.1
- blackducksoftware/blackduck-postgres-waiter:1.0.18
- blackducksoftware/blackduck-cfssl:1.0.34
- blackducksoftware/blackduck-nginx:2025.10.1
- blackducksoftware/blackduck-logstash:1.0.45
- blackducksoftware/bdba-worker:2025.9.1
- blackducksoftware/rabbitmq:1.2.48
- blackducksoftware/blackduck-authentication:2025.10.1
- blackducksoftware/blackduck-bomengine:2025.10.1
- blackducksoftware/blackduck-documentation:2025.10.1
- blackducksoftware/blackduck-integration:2025.10.1
- blackducksoftware/blackduck-jobrunner:2025.10.1
- blackducksoftware/blackduck-redis:2025.10.1
- blackducksoftware/blackduck-registration:2025.10.1
- blackducksoftware/blackduck-scanmatch:2025.10.1
- blackducksoftware/blackduck-storage:2025.10.1
- blackducksoftware/blackduck-webapp:2025.10.1

API Enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

There are no new API enhancements in 2025.10.1.

Binary Scanner Information

The binary scanner has been updated to version **2025.9.1**.

Fixed Issues

The following customer-reported issues have been fixed in this release:

- (HUB-44483). Fixed an intermittent issue where 'Component Link' information was missing in Black Duck SCA reports, improving reliability for licensing and audit workflows. The fix ensures consistent link data across environments and versions.

- (HUB-44625). Fixed issues with stuck LTS transition jobs and failed rescans after upgrade, improving reliability of long-term support version conversions and preventing failures caused by database conflicts and residual data.
- (HUB-45472). Fixed an issue preventing updates to component origins for multi-origin components, ensuring consistent UI behavior and successful origin adjustments by removing legacy origin data and supporting only a single origin after changes.
- (HUB-45687). Fixed a license database access issue causing 400 errors in Black Duck SCA on-premises deployments, ensuring successful project creation and scans by improving header handling and configuration for secure connections.
- (HUB-45709). Fixed an issue where PURLs were modified during SBOM imports (especially for Golang components), ensuring user-defined PURLs are preserved and prioritized for accurate display and export.
- (HUB-45734). Fixed inconsistent BOM results for NPM packages by aligning fuzzy matching behavior between HUB and SCASS, improving handling of unknown versions, and adding configuration options for better accuracy across all scan paths.
- (HUB-45873). Fixed an issue where versions for the googleapis/go-genproto component were not detected in scans, improving signature matching to ensure accurate version identification for subcomponents.
- (HUB-46114). Fixed an issue where bulk editing the 'Usage' field on SBOM components did not update correctly, ensuring accurate updates for all usage types, including “Dynamically Linked,” in both UI and backend.
- (HUB-46306). Fixed an issue where Path and Archive Context fields were missing in source reports, ensuring all relevant scan data columns are correctly populated for accurate reporting.
- (HUB-46439). Fixed an issue where SBOM components identified only by CPE references were not logged during import, ensuring all components generate BOM Import Log entries with clear status messages for improved visibility.
- (HUB-46467). Resolved an issue in the notifications API where duplicate notifications caused inconsistent results when retrieving notification data. The problem arose from the handling of notifications with identical timestamps, leading to some expected notifications not being returned.
- (HUB-46573). Fixed an issue where SBOM uploads using CycloneDX v1.5 failed due to unsupported tools.services format, adding compliance with the current CycloneDX specification for Tools metadata.
- (HUB-46674). Resolved an issue causing SBOM scans to fail with an "ERR05_1022 Internal Server Error" due to empty Component Hash arrays. The fix ensures that the import process handles such cases more robustly, preventing failures when valid SBOMs contain empty arrays.

Black Duck SCA 2025.10.0

Announcements

Consolidation of Scan and Matchengine Containers

In the 2025.10.0 release, we have merged the `scan` and `matchengine` containers into a single `scanmatch` container. This change is part of our ongoing efforts to reduce resource requirements for Black Duck SCA deployments, enhancing efficiency and performance.

NOTE: Moving to the consolidated scanmatch container will require transitioning to Gen05 SPH hardware configurations.

PostgreSQL 17 Production Support Update

We would like to inform our users that we will not be providing production support for PostgreSQL 17. Instead, we will be skipping PG 17 and redirecting our efforts towards enhancing evaluation support for PostgreSQL 18. This decision reflects our commitment to ensuring that our customers have access to the most stable and effective database solutions. Thank you for your understanding as we strive to improve your experience with our products.

PostgreSQL container migration to version 16

With the release of Black Duck SCA 2025.10.0, the PostgreSQL image will be upgraded to version 16. Customers who are not using the Black Duck-supplied PostgreSQL image will not be affected.

End of Support for PostgreSQL 15

With the release of Black Duck SCA 2025.10.0, support for external PostgreSQL 15 will be discontinued. For more information, please refer to the PostgreSQL Version Upgrade Schedule.

Upgrade restrictions for PostgreSQL container users

For users of the Black Duck-provided PostgreSQL container, Black Duck SCA supports direct upgrades only from earlier versions that use PostgreSQL 14 or 15 (specifically, version 2023.10.0 and later).

Upgrading from older Black Duck SCA versions (prior to 2023.10.0) will require a multi-step process:

- From version 2021.10.0 and earlier: Upgrade from the currently installed version to 2023.7.x, then to 2025.7.x, and finally to 2025.10.0.
- From versions 2022.2.x through 2023.7.x (inclusive): Upgrade from the currently installed version to 2024.7.x, then to 2025.10.0.

New and changed features

AI Model Support in Bill of Materials

Black Duck now supports the addition of AI models to your Bill of Materials (BOM) as part of the Black Duck Supply Chain Edition, enabling comprehensive tracking and management of artificial intelligence components within your projects. This new feature allows organizations to maintain visibility into their AI model usage alongside traditional software components.

Key capabilities include:

- Manual addition and editing of AI models to your BOM with detailed metadata
- Filtering and search options to quickly identify AI models within large BOMs

Note: This feature is currently available only for hosted customers, as it requires signature scans to be processed through the SCA Scan Service (SCASS).

To use this feature, ensure your product registration has the AI Model Scanning feature enabled and run Detect scans with the parameter `--detect.blackduck.signature.scanner.individual.file.matching=ALL`.

This enhancement helps organizations address the growing need to track AI components as part of their software supply chain management and compliance processes.

New BDSA Rapid Review tag

With the introduction of AI assistance for generating fully automated BDSAs without human research, we have introduced a new BDSA tag called "Rapid Review." This tag alerts users to potential vulnerabilities

identified through our automated vulnerability process, which was partly developed in response to the need for timely reporting of Linux Kernel vulnerabilities.

You will find the Rapid Review tag in all areas where other vulnerability tags are found:

- Project and vulnerability pages
- Support on the Find page
- Conditions for policy violations
- Filter conditions for the vulnerabilities page

New Vulnerabilities Dashboard

Black Duck SCA 2025.10.0 introduces the New Vulnerabilities Dashboard, which provides users with an enhanced view of vulnerabilities detected within their projects. This dashboard features a comprehensive overview of new vulnerabilities, allowing users to filter by timeframe and access detailed information about affected projects. With an intuitive layout and graphical summaries of vulnerabilities by severity, the New Vulnerabilities Dashboard streamlines the vulnerability management process, making it easier for users to prioritize remediation efforts.

New Component search functionality for LTS Projects

We have introduced the ability to search for components within Long-Term Support (LTS) project versions in Black Duck SCA. Customers can now perform the same search capabilities for components in LTS projects as they can for active projects.

When searching for components, the results will now include relevant LTS project versions, ensuring that all affected components are considered in your queries. This enhancement aims to improve the effectiveness of component management across different project types.

New Vulnerability Exploitability eXchange (VEX) Reports

The new Vulnerability Exploitability eXchange (VEX) reports are now available in Black Duck SCA as part of the Black Duck Supply Chain Edition. These reports provide a standardized method for communicating the exploitability status of vulnerabilities associated with your products.

Users can generate VEX reports in the CSAF 2.0 (Profile 5) format, which includes key metadata such as the CVE ID (if available), BDSA ID, and vulnerability ratings. The reports will only include vulnerabilities that are relevant, filtering out those marked as Duplicate, Ignored, or New.

VEX reports can be generated through the user interface or via API, allowing for flexibility in accessing vulnerability information. This feature aims to help organizations communicate security risks more effectively and enhance their vulnerability management processes.

To take advantage of this new report, ensure your product registration has the Vulnerability Exploitability eXchange (VEX) feature enabled.

Enhanced Vulnerability Information in SBOM Reports

Black Duck now provides enhanced vulnerability information in both SPDX 3 and CycloneDX SBOM reports, enabling more comprehensive security insights for stakeholders. This update filters out vulnerabilities with "Duplicate," "Ignored," or "New" remediation statuses, ensuring reports focus on the most relevant security information.

For CycloneDX reports, we've added detailed vulnerability ratings with scoring methods and vectors, Common Weakness Enumeration (CWE) listings, and analysis information including state, justification, and response details. SPDX 3 reports now include vulnerability classes with CVE or BDSA IDs, CVSS assessment relationships across multiple versions, and specific vulnerability remediation representations.

These improvements align with industry standards and help organizations provide more detailed security context in their software supply chain documentation.

Update to SPDX License Handling in BD SBOMs

We have updated the license handling for Black Duck SBOMs to ensure compliance with the latest SPDX license identifiers. With this change, if a license ID in the SBOM is not part of the supported license list, it will be treated as a custom license, requiring a license reference and inclusion of the full license text. This enhancement is designed to prevent failures during SBOM validation.

Both CycloneDX and SPDX rely on the license identifiers defined in the SPDX License List. It is important to note that, following the transition from SPDX 2.3 to SPDX 3.0, several license formats were changed, and some licenses were marked as deprecated. While these deprecated licenses currently result in warnings but are still processed as valid SBOMs, they may be removed in future updates, leading to invalid SBOMs.

This update reinforces our commitment to maintaining the integrity and compliance of SBOMs within Black Duck SCA.

UX/UI Enhancements to Project Settings/Details Page

The Project Settings/Details page has been significantly improved with several user experience enhancements designed to streamline navigation and configuration:

- **Reorganized Layout:** Straightforward project details (such as Name and Description) are now separated from more advanced features (such as Custom Scan Signature), creating a more intuitive workflow.
- **Enhanced Documentation:** "Learn More" links have been added throughout the settings and options, providing immediate access to relevant documentation and guidance.
- **Improved Text and Instructions:** UI text and explanations have been revised for clarity, making it easier to understand available options and their implications.
- **Refined Visual Elements:** Updates to layout, alignment, spacing, and behavior create a more consistent and polished interface, improving overall usability.

These enhancements aim to streamline project management and make configuration more accessible for both new and experienced users.

LTS BOM Count in Export CSV Reports

A new "LTS BOM Count" column has been added to the Export CSV report available on the Find → Vulnerabilities page. This enhancement allows users to easily track the number of Long-Term Support (LTS) Bill of Materials (BOM) components associated with identified vulnerabilities. By including the LTS BOM Count in the exported reports, users can gain better insights into their LTS components and enhance their vulnerability management processes.

Minimum supported browser versions

- Safari Version 17.1
- Chrome Version 119 (x86_64)
- Firefox Version 119 (64-bit)
- Microsoft Edge Version 119 (64-bit)

Container versions

- blackducksoftware/blackduck-postgres:16-2.5

- blackducksoftware/blackduck-postgres-upgrader:16-1.1
- blackducksoftware/blackduck-postgres-waiter:1.0.18
- blackducksoftware/blackduck-cfssl:1.0.34
- blackducksoftware/blackduck-nginx:2025.10.0
- blackducksoftware/blackduck-logstash:1.0.45
- blackducksoftware/bdba-worker:2025.9.1
- blackducksoftware/rabbitmq:1.2.48
- blackducksoftware/blackduck-authentication:2025.10.0
- blackducksoftware/blackduck-bomengine:2025.10.0
- blackducksoftware/blackduck-documentation:2025.10.0
- blackducksoftware/blackduck-integration:2025.10.0
- blackducksoftware/blackduck-jobrunner:2025.10.0
- blackducksoftware/blackduck-redis:2025.10.0
- blackducksoftware/blackduck-registration:2025.10.0
- blackducksoftware/blackduck-scanmatch:2025.10.0
- blackducksoftware/blackduck-storage:2025.10.0
- blackducksoftware/blackduck-webapp:2025.10.0

API enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Public hierarchical BOM APIs to return HTTP 410 Gone

The following APIs have been sunset and now return HTTP 410 Gone. The associated REST API documentation for these endpoints have also been removed:

- `GET /api/projects/{projectId}/versions/{projectVersionId}/hierarchical-components`
- `PUT /api/projects/{projectId}/versions/{projectVersionId}/hierarchical-components`
- `GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/hierarchical-components/{hierarchicalId}/children`
- `GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/hierarchical-components/{hierarchicalId}/children`

Behavior Change in Component Vulnerabilities API

As a follow-up to the deprecation announced in 2025.7.0, the `GET /api/components/<component-id>/vulnerabilities` API endpoint has been modified in version 2025.10.0 to limit results to the first 10 component versions' vulnerabilities. This change serves as a performance protection measure for the system.

Please note that this API remains deprecated and is scheduled for removal in version 2026.1.0. Users are strongly encouraged to transition to the following API endpoints:

- `GET /api/components/<component-id>/versions/<version-id>/vulnerabilities`
- `GET /api/components/<component-id>/versions/<version-id>/origin/<origin-id>/vulnerabilities`

These endpoints provide more accurate and efficient access to vulnerability data for specific component versions and origins.

Upcoming Deprecation of Update Access Token API

In the 2026.1.0 release, the Update Access Token API (`PUT /api/current-user/tokens/{tokenId}`) will be deprecated as part of our ongoing security improvements. After this change, users will no longer be able to update metadata for existing access tokens.

Users will still be able to:

- Create new access tokens with appropriate metadata
- Regenerate new access tokens
- Delete existing tokens

If you need to modify metadata for an existing token, the recommended approach will be to delete the existing access token and create a new one with the required metadata.

This change enhances our security posture while maintaining essential token management functionality.

REST API Documentation for Vulnerability Count Views

We have introduced three new endpoints that allow customers to retrieve additional information from the Black Duck SCA system. These endpoints provide summarized data, including vulnerability counts and projects with vulnerable components, based on a specified time range:

- **Get a vulnerability digest summary:**

  `GET /api/vulnerabilities-digest-summary`
- **Get the vulnerability digest:**

  `GET /api/vulnerabilities-digest`
- **Get the project vulnerability digest:**

  `GET /api/project-vulnerabilities-digest`

Binary scanner information

The binary scanner has been updated to version **2025.9.1**.

Fixed issues

The following customer-reported issues have been fixed in this release:

- (HUB-36738). Resolved a bug in Black Duck SCA versions 2022.7.x and 2022.10.x that caused re-scanning projects with backslash syntax to fail with a "412 Precondition Failed" error; upgrading to Black Duck SCA 2025.10.0 allows successful re-scans with such project names.
- (HUB-43219). Addressed a bug causing unmatched SBOM components to display blank names and missing version info after import; initial fixes have been implemented, with further updates planned for the 2025.10.0 release to improve the handling and editing of unmatched components.

- (HUB-44281). Updated the REST API documentation to remove references to the Hierarchical BOM (HBOM) feature, which is no longer offered.
- (HUB-44483). Resolved a bug causing intermittent missing Component Link information in generated reports in Black Duck SCA, affecting versions 2024.7.3, 2024.10.1, and later; a temporary workaround involving database modifications and service restarts has been identified.
- (HUB-44511). The Integrations Manager role in Black Duck SCA was unable to manage SCM integrations, as it could only manage the Artifactory integration. This functionality has now been corrected to ensure that the Integrations Manager role can manage SCM onboarding configurations, aligning with expectations for role responsibilities.
- (HUB-44558). Resolved a "412 Precondition Failed" error when adding different versions of the same project to a Bill of Materials (BOM), which arose from overly restrictive cyclic dependency detection; the fix removes the restrictive check and implements improved cycle detection, addressing legitimate use cases for customers using multiple project versions.
- (HUB-44580). Fixed an issue where Detect Desktop scans failed with the error message "Request authentication failed" due to a trailing slash (/) in the blackduck_url, which caused authentication failures during scans.
- (HUB-44817). Resolved an issue where user sessions did not expire after the configured timeout of 1800 seconds, causing security concerns; the issue was linked to browser session cookies not expiring.
- (HUB-44895). Fixed an issue where users with the project-level Project Manager role could incorrectly assign any project-level user roles (including Project Administrator) to themselves and others.
- (HUB-44558). Resolved a bug that resulted in a 412 error when attempting to add a different version of a project to the Bill of Materials (BOM) of another version of the same project. This issue blocked valid use cases, particularly for customers who utilize multiple versions of the same project in their BOMs, such as in microservices architectures. The problem originated from a fix designed to prevent projects without versions from being added to BOMs; however, it unintentionally restricted the addition of different versions of the same project. The team has decided to remove this restrictive check, allowing for the addition of different project versions without causing unnecessary upgrade friction. Cyclic dependency detection will continue to be enforced to prevent recursive references, ensuring a balance between functionality and safety.
- (HUB-45006). Resolved a bug where Japanese characters in uploaded source code were not displayed properly due to encoding issues; the root cause was identified as the backend storage service returning raw bytes without encoding info.
- (HUB-45115). Resolved a bug preventing users with the Project Code Scanner role from mapping or unmapping projects as expected, due to backend permission checks on the codelocation API; UI improvements and API enhancements were implemented to clarify scan access post-unmap. A warning is now displayed in the UI before unmapping to inform users about potential access loss.
- (HUB-45186). Resolved an issue where the view for policy violations did not accurately reflect unfulfilled licenses in the component version view.
- (HUB-45308). Resolved a bug causing mismatches in vulnerability counts between the upgrade guidance and component details pages, where UI icons inaccurately displayed vulnerabilities.
- (HUB-45356, HUB-45541, HUB-46005). Fixed additional cases of security risk count discrepancies.
- (HUB-45396). Resolved a bug in SBOM import where the '+' character in PURLs was incorrectly encoded as '%20' instead of '%2B', leading to unmatched components; the root cause was a flaw in the package URL library, which has been fixed by updating to a new dependency version.
- (HUB-45399). Resolved a connectivity bug in Docker Swarm environments where Black Duck SCA could not connect to an external PostgreSQL database, with SSL mode enabled or disabled; the issue was traced to incorrect SSL certificate path settings and permissions. A fix was implemented by adding

a new docker-compose.externaldb-cert-volume.yml for proper certificate volume mounting and adjusting the HUB_POSTGRES_SSL_MODE variable.

- (HUB-45434). Addressed an API bug where deleting an LTS version via the general version delete endpoint returned a 204 No Content response instead of a 4xx error; this behavior led to inconsistencies where the version appeared deleted in the UI but remained in the database. The fix ensures that attempts to delete or manipulate an LTS version using the incorrect endpoint will be rejected, providing an appropriate error response instead.
- (HUB-45472). Resolved an issue where adjustments to component matches were indicated as successful in the UI, displaying the message "The component changes were successfully saved," and returning a status 200 for the PUT request. However, the edits were not being applied as expected. This issue has been fixed to ensure that component match adjustments are correctly applied.
- (HUB-45488). Resolved a bug causing roles to be duplicated within user groups. This issue stemmed from identical role names for projects and groups in the backend API, leading to inconsistencies. The user interface alone could not address the duplication, necessitating backend changes to differentiate role names—such as adding "Project Group Viewer" to avoid overlaps. Additionally, similar scope-based fixes referenced from a previous issue (HUB-44826) were implemented to further prevent duplication by utilizing role scopes. It was also noted that certain roles, including BOM Annotator, BOM Manager, Policy Violation Reviewer, and Project Code Scanner, were not appearing correctly. This fix ensures accurate role representation and resolves the duplication issue.
- (HUB-45537). Resolved a bug in the binary scan results UI where match type, component name, license, and usage information were not displayed, unlike package manager scans.
- (HUB-45593). Resolved a bug in the search function on the online help page that caused it to become unresponsive and return no results when using the Japanese or Simplified Chinese language setting in the browser.
- (HUB-45605). Resolved a bug where uploading a valid SBOM with no components incorrectly marked the project version as "Never Scanned," causing confusion in reporting; the fix ensures that the scanned timestamp updates correctly even when no PURLs are present.
- (HUB-45617). Fixed an issue where the login page would still appear when the Black Duck SCA was actually down.
- (HUB-45648). Resolved a bug where the system-level project setting for License Conflicts was not inherited when creating a project by uploading BDIO files; unlike projects created through scanning or the UI, the License Conflicts setting was not enabled in the automatically created project. The fix ensures that this setting is now inherited correctly across all project creation methods.
- (HUB-45675). Improved handling of RESERVED CVEs in the Black Duck SCA API by updating UI messaging; previously, a 404 error for RESERVED CVEs was indistinguishable from invalid CVEs. The UI now displays a specific message for RESERVED CVEs when accessed via BDSA links, indicating they are "Reserved but not yet published by the NVD," while direct navigation to invalid CVE URLs presents a generic "not found" message.
- (HUB-45734). Fixed an issue in SCASS-enabled NPM package manager scans that resulted in unexpected and incorrect match results compared to non-SCASS scans. The issue arose due to the use of fuzzy matching in SCASS-enabled scans, which led to incorrect version matches, while HUB's default setting utilized exact matching. Additionally, uploading BDIO files bypassed SCASS, yielding more accurate results than live SCASS scans.
- (HUB-45781). Fixed an issue where unknown licenses did not appear in Notice File reports unless part of an AND/OR clause.
- (HUB-45782). Resolved a bug that prevented users from removing Originator information set for components under 'SBOM Fields'; users could input Originator Entity and Name but were unable to clear these fields upon updating.

- (HUB-45788). Resolved a performance issue where the "Dashboard Summary" page took longer than expected to load all sub-blocks for some customers. The investigation identified that the `GET /internal/dashboard-top-security-risk` endpoint was causing significant delays in page rendering.
- (HUB-45835). Resolved documentation errors in the Black Duck SCA User Guide, including adjustments to snippet matching size, BOM/JSON file naming, and project creation instructions. The maximum snippet size is now correctly stated as adjustable between 1-4 MB with a default of 1 MB. Outdated BOM/JSON naming instructions were removed, and project creation clarity was improved based on SCM integration status.
- (HUB-45851). Clarified the behavior of the "Component Adjustments" setting in project versions by updating the UI text to accurately reflect that adjustments apply across all project versions where the component exists, while manually added components must be handled individually. The revised description and a proposed "Learn More" link to documentation enhance user understanding.
- (HUB-45868). Resolved a bug that caused the average signature scan size metric to display as 0.0 MB in system usage reports due to incorrect data reading in the backend, confirmed as an API issue related to improper SQL result indexing. The fix corrects the query for reading monthly scan statistics, with updates scheduled for releases in 2025.10.0 and 2026.1.0.
- (HUB-45873). Resolved a bug where no versions were detected for the googleapis/go-genproto component in scanned Docker container binaries; the issue stemmed from a bug in signature generation that incorrectly identified the parent component alongside the correct subcomponents.
- (HUB-45886). Resolved a problem with Black Duck's data retention settings that incorrectly triggered premature unmapping of scans following manual .BDIO file uploads. The issue was identified when data retention rules activated immediately after uploads, disrupting workflows. The fix ensures that data retention policies now consider manual uploads, preventing premature unmapping and aligning with expected behavior.
- (HUB-45970). Resolved a bug that allowed the creation of selector-type custom fields with zero options, leading to UI crashes on component version custom fields pages. The issue was caused by the backend API returning an empty options array for these fields, affecting all component versions since version 2019.2.0. The fix disallows the creation of selector custom fields without options, improving UI stability. A temporary workaround involved disabling or adding options to existing custom fields.
- (HUB-45975). Resolved a "Duplicate Key" error on the Issues endpoint caused by multiple BOM entries with the same component/version IDs but different names. The root cause was identified as KB component name changes not being handled in the KBUpdate Job, leading to conflicts in the version_bom_component table.
- (HUB-45977). Resolved a bug where editing a snippet on the Source page resulted in the snippet count being incorrectly doubled upon rescanning; this caused the system to display 4 matches for the edited snippet instead of the expected 2. The issue arose from the system summing file adjustments or counting them twice per scan. The fix ensures that snippet matches are accurately counted during rescans, maintaining consistent match counts across versions.
- (HUB-45979). Resolved an issue where the `vulnerable-bom-components` API endpoint incorrectly displayed components that have been removed from layers in a container scan.
- (HUB-46073). Resolved a bug where binary scan results displayed extra components in the Source tab, leading to confusion for users. The issue involved two DLL files showing an unexpected number of component matches, particularly when selecting "All Subfolders" in the Source tab, which incorrectly added extra components not linked to the BOM. The fix ensures accurate representation of components in the Source tab, aligning with expected results observed in standalone binary scans.

- (HUB-46084). Resolved a bug in the /source-trees API endpoint where pagination parameters (?limit, offset) stopped working after Black Duck 2025.1.1, disrupting customer workflows. The issue was traced to the UI not passing the limit parameter due to a refactor.
- (HUB-46126). Resolved a bug where ignored snippet matches caused license conflicts in a main project after scanning a subproject. The issue arose when GPL-licensed snippets from external projects were ignored during the subproject scan, but their licenses carried over and caused conflicts in the main project with a non-GPL proprietary license.
- (HUB-46132). Addressed an intermittent scan failure issue where scans returned a "NOT_INCLUDED" status due to the deletion of redundant scans before Detect could request BOM status.
- (HUB-46133). Resolved a bug that caused a 400 Bad Request error when cloning project versions with over 500 distinct component versions containing vulnerability remediations in Black Duck SCA. The issue stemmed from a SQL query exceeding column limits, leading to an "index out of range" exception.
- (HUB-46139, HUB-46164, HUB-46194). Clarified the documentation to specify the use of `scass.blackduck.com` as the SCASS Hostname for proper configuration. Added details on SCASS communication security, confirming that no changes have been made to the transmitted data, only to internal query processing. Expanded the documentation to outline the benefits and disadvantages of SCASS, noting that while SCASS scans may appear slower, they significantly reduce resource requirements for non-specialized scanning. Additionally, referenced Gen05 hardware scaling guidance, highlighting that Gen05 requires about 25% less hardware for the same scan volume compared to Gen04, reflecting the improvements in SCASS.
- (HUB-46144). Resolved a bug in container scans where components were incorrectly shown as both added and removed in the same base layer, leading to discrepancies in component listings. The issue was observed when scanning base images separately compared to their use in derived images, specifically affecting components like the GNU C Library. The fix ensures accurate representation of components across scans, eliminating confusion in the results.
- (HUB-46154). Resolved a discrepancy in snippets count displayed between the BOM page and the Source View; the mismatch occurred due to the aggregation of snippet matches for files with multiple snippets linked to different components. The fix ensures that when sorting by component or license, entries for files with multiple snippets are split into separate rows, accurately reflecting the total snippet count.
- (HUB-46182). Resolved an issue that caused delays in processing changes to project version custom fields. The computation for these changes is now handled as a background process, significantly improving response times and overall efficiency.
- (HUB-46260). Resolved an error where snippet scanning returned "ERR01_1001 Server returned an error (Bad Request)" when scanning from folders with spaces in their names. This fix ensures that folders such as "Test Scan" can be scanned successfully without encountering errors.
- (HUB-46324). Improved efficiency in the KB update workflow by addressing the performance issue with the ProjectGroupCacheRepository, which was causing slowdowns during scans.

Black Duck SCA 2025.7.x

Black Duck SCA 2025.7.1

Announcements

There are no announcements for Black Duck SCA 2025.7.1.

New and changed features

There are no new or changed features in Black Duck SCA 2025.7.1.

API enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

There are no API changes in Black Duck SCA 2025.7.1.

Binary scanner information

The binary scanner has been updated to version **2025.6.3**.

Fixed issues

The following customer-reported issues have been fixed in this release:

- (HUB-44558). Resolved a bug that resulted in a 412 error when attempting to add a different version of a project to the Bill of Materials (BOM) of another version of the same project. This issue blocked valid use cases, particularly for customers who utilize multiple versions of the same project in their BOMs, such as in microservices architectures. The problem originated from a fix designed to prevent projects without versions from being added to BOMs; however, it unintentionally restricted the addition of different versions of the same project. The team has decided to remove this restrictive check, allowing for the addition of different project versions without causing unnecessary upgrade friction. Cyclic dependency detection will continue to be enforced to prevent recursive references, ensuring a balance between functionality and safety.
- (HUB-46221, HUB-46224). Custom field options created prior to version 2025.7.0 were not properly migrated to match the format required by the 2025.7.0 codebase. A new migration script has been implemented to automatically upgrade these entries to the correct format. This ensures that all custom field options display and function correctly after upgrading to version 2025.7.0.

  If you have made changes to the custom field values that were not functioning correctly after the 2025.7.0 upgrade, please reach out to Support before applying the 2025.7.1 upgrade. It is necessary to clean up the values in the database prior to the upgrade to prevent any potential failures during the process. Your prompt attention to this matter will help ensure a smooth upgrade experience.

Black Duck SCA 2025.7.0

Announcements

Updated project version BOM view with new Vulnerabilities tab

We have made significant updates to the project version BOM view by replacing the Security tab with a new Vulnerabilities tab. This redesigned tab offers an improved layout while continuing to provide essential vulnerability insights. Users will benefit from enhanced filtering options, clearer presentation of vulnerability data, and quicker access to remediation details in a more intuitive interface.

The new Vulnerabilities tab changes the way vulnerabilities are remediated, allowing for remediation at the component version level. This means there is no longer a need to remediate individual component origins identified from scans, reducing the overall remediation steps required. Additionally, bulk remediation of multiple vulnerabilities affecting one or more component versions is now supported.

We are also introducing new public vulnerability APIs to facilitate this functionality for customers looking to automate remediation steps. The existing APIs will remain available and have not been deprecated, but we encourage customers to consider transitioning to the new, more efficient APIs that focus on

component version-level remediation. Existing remediation for component origins will be carried forward when upgrading to version 2025.7.0.

Upcoming PostgreSQL container migration to version 16

Starting in **2025.10.0**, Black Duck will upgrade the PostgreSQL container image to PostgreSQL 16. This migration ensures improved performance, stability, and access to the latest PostgreSQL features. Customers using the packaged PostgreSQL container should validate their environments for compatibility with PostgreSQL 16 prior to upgrading. No action is required for those using external databases.

Upcoming upgrade restriction for PostgreSQL container users

Starting in **2025.10.0**, Black Duck will only support direct upgrades to the bundled PostgreSQL container (PostgreSQL 16) from versions that already use PostgreSQL 14 or 15—specifically, Black Duck 2023.10.0 through 2025.7.x.

If you are using a Black Duck version prior to 2023.10.0, you will need to perform a two-step upgrade:

1. First upgrade to 2024.7.x
2. Then upgrade to 2025.10.x

This change applies only to users of the Synopsys-provided PostgreSQL container. Users with external database configurations are not affected.

Upcoming end of support for PostgreSQL 15

Support for **PostgreSQL 15** will end with the **2025.10.0** release of Black Duck.

Users currently using the PostgreSQL 15 container should plan to upgrade to PostgreSQL 16 by of before that release.

External database configurations should follow standard compatibility guidance.

Extended Testing Period for PostgreSQL 17 Support

Black Duck is extending the testing-only period for PostgreSQL 17 as an external database option due to a discovered performance degradation with PG 17.x. While our investigation is ongoing to resolve this issue, we do not recommend using PG 17.x in production environments at this time. Therefore, evaluation-only support for PG 17.x has been extended.

Please note, this extension does not affect our planned end of support for PostgreSQL 15.x, which will occur with the release of Black Duck 2025.10.0. Stay tuned for further updates as we work towards full production support for PostgreSQL 17.x in future releases.

New requirement: `pg_trgm` extension for PostgreSQL

Starting in Black Duck 2025.7.0, the `pg_trgm` PostgreSQL extension is required for the `bds_hub` database.

- If you are using the Black Duck-provided PostgreSQL container, no action is required—the extension will be installed automatically during the upgrade.
- If you are using an external PostgreSQL instance, the upgrade process will attempt to install the extension. However, this may fail in environments with restricted permissions (such as Amazon RDS or other managed services).

To avoid migration issues, Black Duck strongly recommends ensuring that the `pg_trgm` extension is installed in the `bds_hub` database before upgrading to 2025.7.0.

- For managed services, refer to your provider's documentation for instructions on enabling database extensions.
- For standard PostgreSQL installations, you can manually install the extension using:

```
CREATE EXTENSION IF NOT EXISTS pg_trgm;
```

Upcoming scan and matchengine container merger

In the 2025.10.0 release, the `scan` and `matchengine` containers will be merged into a single `scanmatch` container. This change is part of ongoing efforts to reduce resource requirements and simplify Black Duck SCA deployments.

Upcoming scan endpoint deprecations

To improve maintainability and streamline the Black Duck API, several legacy scan-related endpoints are scheduled for deprecation in upcoming releases. The table below outlines the endpoints affected, along with their deprecation timelines.

- Only the specifically listed scan types are affected for the endpoints that support multiple scan types.
- Customers using any of the affected endpoints are encouraged to contact their account team or Technical Support for assistance or migration guidance.

Customers using a fully supported version of Detect (9, 10) at the time of API removal will not be affected and do not need to take any action. None of the supported Detect versions rely on the APIs scheduled for removal in 2026.4.0. By 2027.4.0, Detect 11 will be the oldest supported version, and it does not use any of the deprecated APIs. For more information, see Black Duck Detect end of support and service schedule.

API Endpoint	Content Type	Deprecated With	Removed With	Scan Types
`POST /v1/scans`	*NULL, application/vnd.blackducksoftware.internal-cli-1*	2025.7.0	2026.4.0	• Package Manager • Signature
`PUT /v1/scans/{scanId}`	*NULL, application/vnd.blackducksoftware.internal-cli-1*	2025.7.0	2026.4.0	• Package Manager • Signature
`POST /bom-import`	*application/ld+json*	2025.7.0	2028.1.0	• Package Manager • Signature
`POST /intelligent-persistence-scans`	*application/vnd.blackducksoftware.intelligent-persistence-scan-1-ld-2+json* *application/vnd.blackducksoftware.intelligent-persistence-scan-2-ld-2+json* *application/vnd.blackducksoftware.intelligent-persistence-scan-3+protobuf*	2025.7.0	2027.4.0	• Package Manager • Signature • Binary • Container

`PUT /intelligent-persistence-scans/{scanId}`	*application/vnd.blackducksoftware.intelligent-persistence-scan-1-ld-2+json* *application/vnd.blackducksoftware.intelligent-persistence-scan-2-ld-2+json* *application/vnd.blackducksoftware.intelligent-persistence-scan-3+protobuf*	2025.7.0	2027.4.0	• Package Manager • Signature • Binary • Container
`POST /uploads`	*multipart/form-data*	2025.1.0	2027.4.0	• Binary
`POST /uploads/multipart`	*application/vnd.blackducksoftware.binary-multipart-upload-start-1+json*	2025.1.0	2027.4.0	• Binary
`PUT /uploads/multipart/{scanId}`	*application/vnd.blackducksoftware.multipart-upload-data-1+octet-stream*	2025.1.0	2027.4.0	• Binary
`POST /uploads/multipart/{id}/completed`	*application/vnd.blackducksoftware.multipart-upload-finish-1+json*	2025.1.0	2027.4.0	• Binary
`POST /storage/containers/{scanId}`	*application/vnd.blackducksoftware.container-scan-data-1+octet-stream*	2025.1.0	2027.4.0	• Container
`POST /storage/containers/{id}/message`	*application/vnd.blackducksoftware.container-scan-message-1+json*	2025.1.0	2027.4.0	• Container
`POST /storage/containers/{id}/multipart`	*application/vnd.blackducksoftware.multipart-upload-start-1+json*	2025.1.0	2027.4.0	• Container
`PUT /storage/containers/{id}/multipart`	*application/vnd.blackducksoftware.multipart-upload-data-1+octet-stream*	2025.1.0	2027.4.0	• Container
`POST /storage/containers/{id}/multipart/completed`	*application/vnd.blackducksoftware.multipart-upload-finish-1+json*	2025.1.0	2027.4.0	• Container

New and changed features

New integration support for GitHub App

Black Duck now supports integration with the new GitHub App, a new SCM onboarding application designed to simplify and automate the process of connecting GitHub to Black Duck. Once integrated, the GitHub App performs scans and send results directly to Black Duck, enabling streamlined onboarding and centralized visibility into open source risk. For setup details and configuration guidance, see GitHub App Integration Guide.

Added support for SPDX v3.0

Black Duck now supports both importing and exporting Software Bill of Materials (SBOMs) in the SPDX v3.0 format. This allows greater compatibility with modern tooling and enhanced SBOM data structure support.

For more information about the SPDX v3.0 specification, visit the SPDX v3.0 reference page.

Added support for SBOM Type field in SBOM reports

Black Duck SBOM reports now include a new SBOM Type field that identifies the phase of the software lifecycle the SBOM represents. Supported values are `Design`, `Source`, `Build`, `Analyzed`, `Deployed`, and `Runtime` in alignment with guidance from CISA's SBOM documentation.

This enhancement improves the clarity and traceability of SBOMs by helping consumers understand the context and completeness of the data provided.

New Component Hash support added to SBOMs

Black Duck SBOMs now support a new Component Hash feature that allows users to include a cryptographic identifier for components. When enabled in a SBOM template, users can populate two new fields:

- Hash Value: A unique cryptographic hash value identifying the component's contents.
- Hash Algorithm: The algorithm used to compute the hash value (e.g., SHA-256).

This enhancement improves the traceability and supports integrity verification across SBOMs.

ReversingLabs Functionality Sunset

Support for ReversingLabs functionality has been fully removed from Black Duck. The includes removal of all previously deprecated features, APIs, and schema references related to ReversingLabs. Any public ReversingLabs APIs that remain will now return a `410 Gone` response or are marked as deprecated. As part of this change, all documentation references have also been removed.

If you were using ReversingLabs integrations, we recommend reviewing your workflows and transitioning to supported alternatives.

Updated terminology from "Overall Roles" to "Global Roles"

To improve clarity and consistency across the product, all references to Overall Roles have been updated to Global Roles. This change consolidates terminology and better reflects the scope and function of these roles within Black Duck. Only the name has changed—role functionality and permissions remain the same.

Updated filter behavior to include LTS projects

The Affecting Projects filter on the Find → Vulnerabilities page has been updated to include Long-Term Support (LTS) projects. When enabled, this filter now limits results to vulnerabilities found in both Active and LTS projects, giving users a more complete view of risks affecting supported versions.

New file types supported for snippet scans

Black Duck now supports snippet scanning for Kotlin (.kt) and Rust (.rs) files. These additions expand language coverage and improve identification of code snippets during analysis. No configuration changes are required—scans will automatically detect and process these file types.

Accessibility improvements

This release introduces several updates aimed at enhancing the overall accessibility and usability of Black Duck. These changes improve support for assistive technology and align more closely with accessibility standards such as WCAG.

- Improved Global Search → dropdown menu accessibility.
- Manage and Admin side menus can now be accessed via keyboard.
- Dropdown menus are now navigable by keyboard when expanded and closable when the Escape key. Focus remains within the menu component until it’s closed.
- Improved contrast ratio for scan error messages.
- Improved labeling for SBOM input fields to support better keyboard and screen reader navigation.

Container versions

- blackducksoftware/blackduck-postgres:15-2.4
- blackducksoftware/blackduck-postgres-upgrader:15-2.6
- blackducksoftware/blackduck-postgres-waiter:1.0.18
- blackducksoftware/blackduck-cfssl:1.0.34
- blackducksoftware/blackduck-nginx:2025.7.0
- blackducksoftware/blackduck-logstash:1.0.43
- blackducksoftware/bdba-worker:2025.3.1
- blackducksoftware/rabbitmq:1.2.46
- blackducksoftware/blackduck-authentication:2025.7.0
- blackducksoftware/blackduck-bomengine:2025.7.0
- blackducksoftware/blackduck-documentation:2025.7.0
- blackducksoftware/blackduck-integration:2025.7.0
- blackducksoftware/blackduck-jobrunner:2025.7.0
- blackducksoftware/blackduck-matchengine:2025.7.0
- blackducksoftware/blackduck-redis:2025.7.0
- blackducksoftware/blackduck-registration:2025.7.0
- blackducksoftware/blackduck-scan:2025.7.0
- blackducksoftware/blackduck-storage:2025.7.0

- blackducksoftware/blackduck-webapp:2025.7.0

API enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Deprecation of the component vulnerabilities API endpoint

The following API endpoint is now marked as deprecated:

- `GET /api/components/<component-id>/vulnerabilities`

To enhance accuracy, vulnerabilities are more effectively mapped to:

- Component versions:

  `GET /api/components/<component-id>/versions/<version-id>/vulnerabilities`

- Component origins:

  `GET /api/components/<component-id>/versions/<version-id>/origin/<origin-id>/vulnerabilities`

As a result, we recommend that customers transition their usage to the documented endpoints for component version vulnerabilities and component origin vulnerabilities. A future version will limit the amount of data returned from the deprecated endpoint, followed by a subsequent version that will fully remove the API. Users are encouraged to update their implementations accordingly to ensure continued access to vulnerability data.

Binary scanner information

The binary scanner has been updated to version **2025.3.1**.

Release highlights and fixed issues

-

Fixed issues

The following customer-reported issues have been fixed in this release:

- (HUB-34976, HUB-39582). Fixed an issue where certain TAR archives could not be unpacked by the scan client. Previously, some TAR files were treated as single files rather than unpacked and scanned properly. The scan client now correctly detects and processes these archives.
- (HUB-38990). Fixed an issue where the Project filter may not return results in the Scan Mapping dialog.
- (HUB-43218). Fixed an issue where the tag:value format was not passing the SPDX ntia-conformance-checker in SBOM reports generated using SPDX 2.3.
- (HUB-43300). Fixed an issue where the `/api/notifications/{notifications id}` did not enforce proper user-based authorization.
- (HUB-43916). Fixed an issue where SCASS scans were not honoring proxy settings.
- (HUB-43992). Fixed a NullPointerException error during Black Duck signature scans caused by a null 'MatchAmbiguityDetail.'
- (HUB-44199). Fixed an issue where users could get an intermittent Unable to manage snippet adjustment error message when using the `PUT /api/projects/{projectId}/versions/{projectVersionId}/bulk-snippet-bom-entries` endpoint.

- (HUB-44217). Fixed an issue where BDMU files larger than 10 MB in size may not be processed by Black Duck.
- (HUB-44246). Updated the Black Duck SCA documentation related to "Hosting location for Black Duck Detect" for Code Sight customers.
- (HUB-44352). Fixed an issue the `st.iscomponentignored` function was not ignoring the `IGNORED_SNIPPET` `ignore_status`.
- (HUB-44469). Removed the dbschema section from the System Information debug page.
- (HUB-44497). Fixed an issue where navigation from an LTS project version returned users ti tge Active Versions tab even when no active versions existed.
- (HUB-44533). Fixed an issue where exact file matching was not enabled when scanning Docker images on Docker version 26 (with '--detect.docker.image') or images created on Docker 26 (with 'detect.docker.tar').
- (HUB-44574). Fixed an issue where match confidence was not returning in package manager scans executed through SCASS.
- (HUB-44586). Fixed an issue where hidden directories (/css/, /js/, /images/, /fonts/) were returning 403 errors instead of 404 errors during DAST scans.
- (HUB-44625). Resolved an issue where project versions remained stuck during conversion to LTS, causing UI spinning and failed rescans due to database conflicts.
- (HUB-44675). Fixed an issue causing intermittent 500 Internal Server Errors during parallel scans on the same code location, due to duplicate key constraint violations in the database.
- (HUB-44684). Improved the performance of project version license term report generation.
- (HUB-44738). Fixed an issue causing duplicate source trees to appear for a single binary scan in Black Duck. The issue, linked to switching from jsonld to protobuf format, has been fixed with code changes and a background job to clean up old scan data.
- (HUB-44807). Fixed an issue in the webapp's risk profile calculation caused by missing cyclic dependency checks in Source View code. The fix prevents adjustments that create direct cyclic references between project versions, ensuring proper error handling and avoiding infinite loops.
- (HUB-44811). Fixed an issue where mapping folders or files to components showed a success message but failed to update the component name in the components tab. The fix disables the Edit button when editing is not allowed and ensures the UI uses the correct PUT API for adjustments.
- (HUB-44844). Fixed an issue where users with the "Project Administrator" or "Project Manager" roles were able to read all users' access tokens via the `GET /api/tokens` endpoint.
- (HUB-44845). Fixed an issue where users with the project-level "Project Administrator" or "Project Manager" roles are able to do BOM comparisons with projects they do not have direct/indirect access to.
- (HUB-44888). Resolved an issue where the component's page did not indicate whether a component was used in Long-Term Support (LTS) projects. This prevented users from identifying which LTS projects were potentially affected by vulnerabilities associated with the component.
- (HUB-44890). Resolved an issue where the 'matched-files' REST API incorrectly counted matches for the same component across multiple scans as one, resulting in mismatched `totalCount` and `items` in the API response.
- (HUB-44923). Fixed an issue where the "Server Unavailable" message could persist on the Black Duck login screen for an extended period after a Docker Swarm deployment had been completed.

- (HUB-44924). Fixed an issue where any authenticated user was able to view the scan summary of a code location via the `GET /api/codelocations/<code-location-id>/scan-summaries` endpoint.
- (HUB-44925). Fixed an issue where CSV exports from certain API endpoint, such as `/api/users`, `/api/risk-profile-dashboard`, and `/api/codelocations`, included user-provided input that could allow formula injection. User input is now properly santized to prevent this behavior. This fix has been applied across all areas of Black Duck where CSVs are generated with user input.
- (HUB-44958). Fixed an issue where attempting to change a component's 'Usage' type (e.g., from "Prerequisite" to "Dynamically Linked") displayed a success message but did not save the changes. The issue was limited to certain 'Usage' types, while others, like "Source Code," worked as expected.
- (HUB-44971). Resolved an issue where users encountered 403 errors during signature scans despite having the project code scanner role assigned. The problem was linked to specific dataset inconsistencies after upgrading from 2024.4.1 to 2025.1.1 and was not reproducible on a clean HUB instance.
- (HUB-45073). Fixed an issue where custom components with Black Duck reference IDs in SBOMs were not auto-created during import, resulting in incomplete BOMs.
- (HUB-45082). Resolved an issue where moving a project group resulted in the removal of its description, displaying "No description." The fix ensures that group descriptions are preserved when groups are moved within the Manage → Project Groups interface.
- (HUB-45087). Fixed an issue where `scan_start_at` was incorrectly mapped in `scan_view` and `scan_stats_view`, using the CL creation time instead of the actual scan start time. This caused all scans on the same CL to share the same start date. The mapping has been corrected to reflect the accurate scan start time.
- (HUB-45100). Fixed an issue where cloning a project version with `update=true` did not preserve the "unknown license" value from the original request.
- (HUB-45112). Fixed an issue where Black Duck failed to process valid CycloneDX 1.4 SBOMs if the "tools" field was missing, despite it not being mandatory per the CycloneDX 1.4 specification. The fix ensures SBOMs without the "tools" field are processed successfully, aligning with the schema requirements.
- (HUB-45139). Fixed a bug where components from BDBA protobuf BDIO scans failed to appear correctly in the HUB UI, unlike JSON BDIO scans. The issue was linked to differences in matching methods and API inconsistencies. The KBAPI 6.2.0 update addressed these matching issues, improving protobuf BDIO component visibility, with ongoing HUB-side fixes required for complete resolution.
- (HUB-45140). Fixed an issue where custom fields added to project conditions in policy rules displayed duplicated values instead of the correct individual entries.
- (HUB-45142). Fixed an issue where certain components from Rocky Linux did not display the correct origin ID or namespace in Black Duck scans.
- (HUB-45167). Fixed an issue in version 2025.1.1 causing SPDX report generation failures when reference locators contained spaces.
- (HUB-45186). Fixed an issue where license fulfillment terms were not correctly reflected in the policy violations view for unfulfilled licenses. Changes made in the legal terms tab did not update the version view, causing inconsistencies between the top-level view and the BOM view. The fix ensures accurate synchronization across views when license terms are marked as fulfilled.
- (HUB-45187). Resolved an issue where cryptography data failed to display unless the component version's approval status was set to 'Unreviewed'. The issue involved incorrect handling of approval statuses other than 'Unreviewed', preventing cryptography data from populating correctly.

- (HUB-45213). Fixed an issue where the match content was missing in the version report for components with Match Type Exact and Binary and File Modified.
- (HUB-45353). Corrected the documentation error regarding the IFM property for creating custom signatures. The documentation incorrectly listed the property as `--blackduck.signature.scanner.individual.file.matching`, which should be `--detect.blackduck.signature.scanner.individual.file.matching`.
- (HUB-45354). Updated the Artifactory plugin installation documentation to replace the outdated sig-repo URL with the correct URL.
- (HUB-45389). Updated the description for Custom Scan Signature to be more inline with its actual functionality.
- (HUB-45396). Resolved an issue where SBOM imports resulted in unmatched components due to incorrect character encoding of '+' in PURLs. The encoding error converted '+' to '%20' instead of '%2B', causing lookup failures. The fix ensures proper encoding, allowing successful PURL lookups and matching of components.
- (HUB-45488). Fixed an issue where roles where duplicated on the User Groups page.
- (HUB-45515). Fixed a signature scan failure (ERR05_1076) experienced by ASML, caused by a NullPointerException in the Hub system. The issue stemmed from a null ScanMatchNode channel version after a MaaS-side fix. The fix involves updating Hub handling of null ScanMatchNode.
- (HUB-45530). Re-enabled source file adjustments for all binary matches and restored functionality as it existed in Black Duck 2024.10.0.
- (HUB-45620). Resolved a bug where comments on components in one child project were incorrectly attributed to all child projects in the parent project's component report. The fix ensures comments are now correctly limited to the child project where they were added.
- (HUB-45659). Fixed a UI issue where a "Failed to load custom fields" banner error appeared on the custom fields page for projects, project versions, components, etc. Despite the error, functionality to view and edit custom fields remained unaffected.

Black Duck SCA 2025.4.x

Black Duck SCA 2025.4.2

Announcements

There are no new announcements for Black Duck 2025.4.2.

New and changed features

There are no new or changed features in Black Duck 2025.4.2.

Container versions

- blackducksoftware/blackduck-postgres:15-2.2
- blackducksoftware/blackduck-postgres-upgrader:15-2.4
- blackducksoftware/blackduck-postgres-waiter:1.0.16
- blackducksoftware/blackduck-cfssl:1.0.32
- blackducksoftware/blackduck-nginx:2025.4.1

- blackducksoftware/blackduck-logstash:1.0.41
- blackducksoftware/bdba-worker:2025.3.0
- blackducksoftware/rabbitmq:1.2.44
- blackducksoftware/blackduck-authentication:2025.4.2
- blackducksoftware/blackduck-bomengine:2025.4.2
- blackducksoftware/blackduck-documentation:2025.4.2
- blackducksoftware/blackduck-integration:2025.4.2
- blackducksoftware/blackduck-jobrunner:2025.4.2
- blackducksoftware/blackduck-matchengine:2025.4.2
- blackducksoftware/blackduck-redis:2025.4.2
- blackducksoftware/blackduck-registration:2025.4.2
- blackducksoftware/blackduck-scan:2025.4.2
- blackducksoftware/blackduck-storage:2025.4.2
- blackducksoftware/blackduck-webapp:2025.4.2

API enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

There are no new or changed API requests in Black Duck 2025.4.2.

Binary scanner information

There are no new or changed features in Black Duck 2025.4.2 for the Binary scanner.

Fixed issues

The following customer-reported issues have been fixed in this release:

- (HUB-45342). Fixed an issue that caused the ignored status flag in `version_bom_risk_warning` to become inconsistent with the remediation status due to residual data in `version_bom_risk_status`. The issue was traced to leftover data in `version_bom_risk_status` from migration scripts, which caused ignored flags to revert incorrectly. The fix involved rerunning migration scripts and deleting specific records where the status was REMEDIATED but ignored was false, ensuring proper synchronization between ignored flags and remediation status.
- (HUB-45481). Resolved an issue where the upgrade to version 2025.4.1 took an excessive amount of time due to an unoptimized upgrade script. The script has been optimized to significantly improve upgrade performance.
- (HUB-45490). Addressed an issue where the KB update job occasionally failed to update certain project versions with newly identified vulnerabilities. During the investigation, it was identified that vulnerability counts for component versions were out of sync across various project versions. As part of this update, the BOM for affected component versions has been refreshed to improve accuracy. However, new components that appear after the BOM refresh are not automatically updated at this time. Further improvements are being actively developed to provide a more comprehensive solution in future releases.
- (HUB-45609). Fixed a SQL error caused by incorrect argument ordering in the query for the endpoint `/api/vulnerabilities/{vulnerability_id}/affected-bom-components`. The issue resulted

in a `BadSqlGrammarException` and a PostgreSQL error indicating a mismatch between the `~~*` operator and argument types (`text` vs. `UUID`). The fix corrected the query's argument order to ensure proper execution across all namespaces.

- (HUB-45699). Improved the performance of the components-in-use API by optimizing the query plan to significantly reduce execution time and resource usage. The previous implementation caused excessive data processing and disk spill during sorting. By streamlining the query logic, the fix greatly reduces system overhead and improves response times, making the API more efficient and usable.

Black Duck SCA 2025.4.1

Announcements

There are no new announcements for Black Duck 2025.4.1.

New and changed features

There are no new or changed features in Black Duck 2025.4.1.

Container versions

- blackducksoftware/blackduck-postgres:15-2.2
- blackducksoftware/blackduck-postgres-upgrader:15-2.4
- blackducksoftware/blackduck-postgres-waiter:1.0.16
- blackducksoftware/blackduck-cfssl:1.0.32
- blackducksoftware/blackduck-nginx:2025.4.1
- blackducksoftware/blackduck-logstash:1.0.41
- blackducksoftware/bdba-worker:2025.3.0
- blackducksoftware/rabbitmq:1.2.44
- blackducksoftware/blackduck-authentication:2025.4.1
- blackducksoftware/blackduck-bomengine:2025.4.1
- blackducksoftware/blackduck-documentation:2025.4.1
- blackducksoftware/blackduck-integration:2025.4.1
- blackducksoftware/blackduck-jobrunner:2025.4.1
- blackducksoftware/blackduck-matchengine:2025.4.1
- blackducksoftware/blackduck-redis:2025.4.1
- blackducksoftware/blackduck-registration:2025.4.1
- blackducksoftware/blackduck-scan:2025.4.1
- blackducksoftware/blackduck-storage:2025.4.1
- blackducksoftware/blackduck-webapp:2025.4.1

API enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

There are no new or changed API requests in Black Duck 2025.4.1.

Binary scanner information

There are no new or changed features in Black Duck 2025.4.1 for the Binary scanner.

Fixed issues

The following customer-reported issues have been fixed in this release:

- (HUB-45290, HUB-45293, HUB-45332, HUB-45360). This release re-addresses an issue where vulnerability remediation status was incorrectly applied to all origins of a component version. The original fix included a database migration and code changes, but remediation statuses could still fall out of sync due to KnowledgeBase update jobs. This update corrects the issue more comprehensively to ensure remediation status is consistently applied per origin.

  Additionally, the database migration script has been updated to prevent subproject risk counts from being reset during the upgrade process. After upgrade, subproject risks may briefly appear missing from project rollups; these values are automatically recalculated by the BOM Vulnerability Recomputation Check within approximately 10 minutes for the server restarting. Once this job is completed, the counts will be updated for subprojects. Archived projects must be unarchived in order to get their BOMs refreshed. Please contact Black Duck customer support for further assistance.

  Note: This fix includes a database migration. For customers with large databases, the migration process may take up to an hour or more to complete.
- (HUB-45300). Fixed an issue where stricter timestamp parsing in the API caused failures when processing issueCreateAt and issueUpdatedAT fields, impacting integrations with issue trackers such as JIRA via Alert 8.0.1. The issue was resolved by introducing a fallback parser to accept additional timestamp formats.
- (HUB-45349). Temporarily removed the vulnerability count label on the Security tab of a component version page. To avoid confusion, the count label has been removed while we address an issue with its accuracy. It may be reinstated in a future release once the issue is resolved.

Known issues

The following is a list of new known issues and limitations in Black Duck SCA:

- In some cases, remediation statuses that initially appear correctly may become out of sync after several days. This issue is believed to be related to automated remediation workflows and affects only certain vulnerabilities. The issue is under investigation.
- In rare cases, a vulnerability's ignored status may not align with its remediation state. Specifically, some vulnerabilities may appear as ignored even when their status is shown as New or Remediation Required. This issue primarily affects older vulnerabilities and is currently under investigation.

Black Duck SCA 2025.4.0

Announcements

Upcoming requirement: `pg_trgm` extension for PostgreSQL

Starting in Black Duck 2025.7.0, the `pg_trgm` PostgreSQL extension will be required for the `bds_hub` database.

- If you are using the Black Duck-provided PostgreSQL container, no action is required—the extension will be installed automatically during the upgrade.

- If you are using an external PostgreSQL instance, the upgrade process will attempt to install the extension. However, this may fail in environments with restricted permissions (such as Amazon RDS or other managed services).

To avoid migration issues, Black Duck strongly recommends ensuring that the `pg_trgm` extension is installed in the `bds_hub` database before upgrading to 2025.7.0.

- For managed services, refer to your provider's documentation for instructions on enabling database extensions.
- For standard PostgreSQL installations, you can manually install the extension using:

```
CREATE EXTENSION IF NOT EXISTS pg_trgm;
```

Preliminary PostgreSQL 17 support

Black Duck 2025.4.0 introduces preliminary support for PostgreSQL 17 as an external database. This support is for **testing purposes only**, and **production use is not supported** at this time. Customers can evaluate PostgreSQL 17 in non-production environments to assess compatibility ahead of future full support.

PostgreSQL images now sourced from Docker Library

Starting in Black Duck 2025.4.0, PostgreSQL images will be sourced from Docker Library instead of Bitnami as the base images for Black Duck's PostgreSQL deployment. This transition occurs automatically and requires no action from users.

HBOM view removed following CVSS 2.0 deprecation

With the removal of CVSS 2.0 support, the HBOM view in Black Duck—previously reliant on CVSS 2.0—will no longer be functional. Customers should use alternative reporting and risk assessment views that support CVSS 3.x and 4.0 for vulnerability prioritization.

Database migration notice

This release includes a database migration related to vulnerability remediation status handling (See HUB-44855 in the Fixed issues section of the release notes for more details). For customers with large databases, the migration process may take up to an hour or more to complete. No action is required, but we recommend planning for additional migration time during the upgrade process.

New and changed features

New MFA secret expiration

Black Duck now enforces a time-to-live (TTL) period for MFA secrets, ensuring they expire after two minutes or when a new secret is requested via the API. IF a user attempts to set up MFA with an expired or invalidated secret, a 401 UNAUTHORIZED error will be returned with an appropriate message. The expiration time is configurable for flexibility.

New BDSA vulnerability tags

Black Duck now includes two new BDSA vulnerability tags to help further classify and assess remote code execution risks:

- **Potential Remote Code Execution**: Flags vulnerabilities that may lead to remote code execution under specific conditions but are not conclusively confirmed.

- **Remote Code Execution Requiring User Input** : Indicates the vulnerability requires user interaction through a user interface to exploit remote code execution.

New policy rule expressions for component and vulnerability age

Black Duck now supports two new policy rule expressions that allow users to define rules based on the age of the components or published vulnerabilities:

- **Component Release Age**: Evaluates the number of days since a component was released. Useful for avoiding newly released components or prioritizing mature libraries.
- **Published Age**: Evaluates the number of days since a vulnerability was published. This can help identify components affected by recently disclosed vulnerabilities.

Both expressions accept a number value in days and compare it against the current date. These additions provide more flexibility when creating time-based risk policies.

 # This feature was suggested by customers. BD-I-13

Added support for supplying external database credentials via predefined secret

Black Duck now supports passing database credentials via user-managed Kubernetes secret when using an external PostgreSQL instance. This allows customers to avoid storing plaintext credentials in the `values.yaml` file.

- A new Helm chart setting, `useHelmChartDbCreds`, has been added. It is enabled `true` by default, preserving the existing behavior where the Helm chart creates the `<name>-blackduck-db-creds` secret using values defined in `values.yaml`.
- Setting this value to `false` allows users to manually create and manage their own `<name>-blackduck-db-creds` secret.
- The user-provided secret must contain the following keys:
  - `HUB_POSTGRES_ADMIN_PASSWORD_FILE`
  - `HUB_POSTGRES_USER_PASSWORD_FILE`
- If the custom secret is invalid or missing, the deployment will fail. The system will not fall back to passwords in `values.yaml`.

For more details and examples, see the Kubernetes installation guide.

 # This feature was suggested by customers. BD-I-7

Added support for Ubuntu 22.04 and 24.04, ending support for Ubuntu 20.04

Starting in Black Duck 2025.4.0, Ubuntu 22.04 and 24.04 are now supported.

As Ubuntu 20.04 reaches end of life on May 31, 2025, Black Duck will remove support for this version in 2025.7.0. Customers using Ubuntu 20.04 should plan to upgrade to a supported version to ensure continued compatibility.

Added support for Docker 26.x

Black Duck now supports Docker version 26.x. This update ensures compatibility with the latest Docker runtime environments and aligns with current container platform standards.

Added PURL filter to BOM component's Origin ID tab

Users can now filter the Origin IDs for a BOM component using PURLs (Package URLs). This enhancements makes it easier to locate and distinguish component identifiers based on standardized package references, improving traceability and SBOM navigation.

Enhanced Vulnerabilities tab for LTS project versions

The Vulnerabilities tab for LTS project versions now includes several updates to improve usability and visibility into risks:

- **New Risk Profile bar** – A visual summary displays the total number of vulnerabilities by severity (Critical, High, Medium, Low), helping users quickly assess the overall security posture of the project version.
- **New search bar and expanded filter** – Users can now:
  - Use the search bar to find specific vulnerabilities by ID, component name, or keyword.
  - Filter vulnerabilities by CWE Tags, Overall Score, Remediation Status, Security Risk, and Vulnerability Tags.

Improved flexibility when importing SBOMs

Black Duck has relaxed strict field requirements when importing SBOM files, improving usability and reducing import errors:

- For CycloneDX reports, if the component name metadata is missing from the report, the import will now succeed. The filename of the SBOM will be used as the scan name in place of the missing metadata.
- For CycloneDX and SPDX reports imported from a BOM project version Scan page, if the report is already mapped to a different project version and the user has permission to access that project version, the error message now clearly displays the conflicting project name and version name, making it easier for users to identify and resolve mapping issues.

  This behavior applies only when importing from the BOM project version Scan page. When importing from the Global Scans page, existing scans with the same name are still replaced automatically—this behavior has not changed.

  There is no change in behavior if the user does not have permission to view the other project version.

Improved performance during bulk policy rule edits

To reduce system load during policy rule editing sessions, Black Duck now limits the number of policy rule messages published to the BOM queue. Previously, a message was published every time a policy rule was saved, even in rapid or bulk editing sessions. This could lead to excessive message generation and downstream performance impacts.

With this update, message publication is intelligently reduced during clustered policy rule edits, helping to improve overall system responsiveness and reduce contention on shared resources such as RabbitMQ and PostgreSQL.

Updated policy violation notification logic

The notification logic for policy violations has been updated to reduce unnecessary alerts. Now, if a user overrides a policy rule violation and the component is later determined to be not in violation, no notification will be sent. Previously, a "policy violation cleared" notification was still triggered, even though the violation had already been overridden.

Updated Users & Groups page display

The Users & Groups page has been updated to display only a user's Global Roles in the Roles column. Previously, this column included roles assigned at the project and group level which lead to duplication in some cases. This update provides a clearer, more accurate view of each user's global access within Black Duck.

Restored file match edits for unmatched binary package manager scan results

In a previous release, binary file match edits were removed for binary scans to address performance issues and improve usability. However, this unintentionally disabled file match edits for unmatched binary package manager scan results, leaving no way to resolve them. This update restores source file edits for these unmatched results, allowing users to properly manage and adjust them.

Minimum supported browser versions

- Safari Version 16.5
- Chrome Version 113 (x86_64)
- Firefox Version 112 (64-bit)
- Microsoft Edge Version 113 (64-bit)

Container versions

- blackducksoftware/blackduck-postgres:15-2.2
- blackducksoftware/blackduck-postgres-upgrader:15-2.3
- blackducksoftware/blackduck-postgres-waiter:1.0.16
- blackducksoftware/blackduck-cfssl:1.0.32
- blackducksoftware/blackduck-nginx:2025.4.0
- blackducksoftware/blackduck-logstash:1.0.41
- blackducksoftware/bdba-worker:2025.3.0
- blackducksoftware/rabbitmq:1.2.44
- blackducksoftware/blackduck-authentication:2025.4.0
- blackducksoftware/blackduck-bomengine:2025.4.0
- blackducksoftware/blackduck-documentation:2025.4.0
- blackducksoftware/blackduck-integration:2025.4.0
- blackducksoftware/blackduck-jobrunner:2025.4.0
- blackducksoftware/blackduck-matchengine:2025.4.0
- blackducksoftware/blackduck-redis:2025.4.0
- blackducksoftware/blackduck-registration:2025.4.0
- blackducksoftware/blackduck-scan:2025.4.0
- blackducksoftware/blackduck-storage:2025.4.0
- blackducksoftware/blackduck-webapp:2025.4.0

API enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Deprecation of v4, v5 data-retention endpoint

Black Duck is deprecating v4 and v5 of the `GET /settings/data-retention` endpoint and introducing v6 as the latest version. Customers are encouraged to transition to v6 to take advantage of the improved functionality, performance, and security enhancements.

Users should update their integrations accordingly, as v4 and v5 will be fully removed in a future release.

Updated `matched-files` API endpoints

A new `strict` parameter has been added to the following API endpoints below.

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

Default value is `strict=true`. When true, the response returns matched files for a component with given component ID, component version ID, and null origin ID. If set to `strict=false`, the response returns matched files for a component with given component ID, component version ID, and arbitrary origin ID.

Binary scanner information

The binary scanner has been updated to version **2025.3.0**.

Release highlights and fixed issues

- (PSC-4557). Linux kernel do not exists in the bdba report.
- (PSC-4602). Alpine distro backport not working for CVE-2025-26519
- (PSC-4595). Visual_studio_runtime not matching version
- (PSC-4582). False version detection - v8 8.17.11.962
- (PSC-4577). Inno Setup binary scanning issue
- (PSC-4553). OpenWRT .ipk packages are not recognized as .debs
- (PSC-4539). ubi file not finding component in PSC/BDBA Binary
- (PSC-4478). Component wrongly identified as Winsparkle
- (PSC-4468). False positive vulnerabilities and 1 component match
- (PSC-4456). File path in cab archives still obfuscated
- (PSC-4452). pe32-fileinfo version data not utilized for signature matches
- (PSC-4231). Binary throwing error while loading in protecodesc production "Scan failed: Unexpected error"

Fixed issues

The following customer-reported issues have been fixed in this release:

- (HUB-34996, HUB-44573). Fixed an issue where the Affected Projects section of the vulnerability details page could fail to load in the UI when a vulnerability was linked to a high number of projects. The underlying API query has been optimized to improve performance, preventing timeouts and ensuring the page loads successfully even for widely shared vulnerabilities.
- (HUB-42633). Optimized the response time for affected-bom-components API endpoint.
- (HUB-42732). Fixed an issue where policy override comments where not properly recorded in the Project Version activity when using the Override All option. Users can now enter individual comments and override expiration per each policy rule.
- (HUB-43377). Fixed an issue where the Reset Adjustment function might not work for manually adjusted entries on the Source page.
- (HUB-43846, HUB-43862). Improved error handling to prevent the creation of circular references. The system now detects and blocks these scenarios to ensure data integrity and avoid processing issues.
- (HUB-43864). Fixed an issue where the policy-status API results did not match the UI. This discrepancy occurred because overridden policy severities were not properly excluded when calculating severity counts.
- (HUB-43972). Fixed an issue where SCASS scans may display the license for components with multiple licenses as UNKNOWN in the lightweight BOM.
- (HUB-44006). Fixed an issue where users with Direct Access (Project Viewer) were unable to view parent project group details on the "Project Group" page.
- (HUB-44177). Fixed an issue where policy violation detection events might not appear in the Activity window after a Policy Approval Updated event was applied to a specific component's policy violation. All relevant policy events are now properly logged and visible in the Activity window.
- (HUB-44178). Fixed an issue where a BOM component with mutliple policy violations did not correctly restore all violations after being unignored.
- (HUB-44274). Fixed an issue where project versions without scans were not deleted by the auto-deletion feature.
- (HUB-44353). Fixed an issue where the Status column on the /api/vulnerabilities/<CVE>/affected-projects page was not working as intended.
- (HUB-44392). Fixed an issue where container scans could display inaccurate build information for each image layer. In certain scenarios, such as images built with Bazel, build steps were offset by one layer, causing each layer to show metadata from the previous layer. This did not affect the accuracy of the scanned contents but may have led to confusion when reviewing layer histories.
- (HUB-44396). Fixed an issue where containers with duplicate layers could generate an `IncorrectResultSizeDataAccessException` error message.
- (HUB-44408, HUB-44590). Fixed an issue where source code containing Japanese and other special characters could not be uploaded, generating a `The content type is not allowed` error message.
- (HUB-44506). Fixed missing "HUB_MAX_MEMORY" variables for containers in Gen05 sizing yaml files.
- (HUB-44551). Fixed an issue when viewing the settings of a project group in which navigating to a new project group’s settings will show the previously viewed project group data.
- (HUB-44604). Fixed an issue when BD is deployed with a time zone setting, the license expiration date's UTC time was being treated as local time, causing it to expire earlier than the actual license time.
- (HUB-44649). Fixed an issue where the number of file matches displayed in Snippet matching was doubled.

- (HUB-44670). Fixed an issue where partially configured mTLS setups could incorrectly treat empty certificate fields as valid, causing unintended behavior during database connection. Only properly configured certificates are now included.
- (HUB-44674, HUB-44970). Fixed an issue where using the `--detect.clone.project.version.name` parameter during a scan did not correctly copy the settings from the specified project version.
- (HUB-44706). Fixed an issue where a NullPointerException error could be generated occured when creating version details report if a vulnerability's CVSS4 vector does not contain a Exploit Maturity value.
- (HUB-44747). Corrected the format of the creators field in the creationInfo section of SPDX SBOMs generated by Black Duck. Previously, the tool name and version were separated by a hyphen without surrounding spaces, which was not compliant with the SPDX specification. The formatting now includes a space on each side of the hyphen as required.
- (HUB-44820). Fixed an issue where Rapid scans could miss certain vulnerabiltiies in some cases. The scoring logic used in Rapid scans has been updated to align with Full scans, ensuring consistent vulnerability detection across scan types—particularly in environments using CVSS v4 or updated ranking configurations.
- (HUB-44853, HUB-44876). Resolved an issue where the Security tab for a component could display a vulnerability count but show "No results" in the list. This was caused by inconsistencies in how the CVSS version was applied when prioritizing vulnerabilities. The display logic has been corrected to ensure vulnerability data is show consistently with the reported count.
- (HUB-44855). Fixed an issue where the vulnerability remediation status was incorrectly applying to all origins of a component version, instead of only the intended one. The system now correctly reflects remediation status per origin. Please note that this fix includes a database migration. For customers with large databases, the migration may take up to an hour or more to complete.
- (HUB-44872). Fixed an issue where users with the Project Manager or Project Administrator roles where not able to delete LTS versions.
- (HUB-44879). Fixed an issue where "Policy Violation Detected" event notifications could re-trigger unexpectedly after re-scanning, causing Alert duplicate JIRA comments to be created.
- (HUB-44889). Fixed the broken Black Duck Tutorials link in the '?' drop down of the UI.
- (HUB-44891). Fixed an issue where components marked as ignored continued to show security risk indicators on the Component tab. Ignored components will now correctly exclude security risk data.
- (HUB-45007). Fixed an issue where users could not save a snippet match without specifying a component version, generating a "Cannot create/modify file adjustment to a project without a version ID" error.

Black Duck SCA 2025.1.x

Black Duck 2025.1.1

Announcements

There are no new announcements for Black Duck 2025.1.1.

New and changed features

Added support for IPv6 ingress and egress communication

Black Duck now supports IPv6-exclusive networks for both internal and external communication. This enhancement ensures compatibility with IPv6-only environments, enabling seamless communication between Black Duck components, the KnowledgeBase, customer systems, and internet-facing networking pods.

Added `justification` field to the `component_vulnerability` table

A new `justification` field has been added to the `component_vulnerability` table in the reporting database. This field store the justification details for vulnerabilities, providing additional context for remediation decisions and analysis.

Container versions

- blackducksoftware/blackduck-postgres:15-1.10
- blackducksoftware/blackduck-postgres-upgrader:15-1.3
- blackducksoftware/blackduck-postgres-waiter:1.0.14
- blackducksoftware/blackduck-cfssl:1.0.30
- blackducksoftware/blackduck-nginx:2025.1.1
- blackducksoftware/blackduck-logstash:1.0.40
- blackducksoftware/bdba-worker:2024.12.2
- blackducksoftware/rabbitmq:1.2.42
- blackducksoftware/blackduck-authentication:2025.1.1
- blackducksoftware/blackduck-bomengine:2025.1.1
- blackducksoftware/blackduck-documentation:2025.1.1
- blackducksoftware/blackduck-integration:2025.1.1
- blackducksoftware/blackduck-jobrunner:2025.1.1
- blackducksoftware/blackduck-matchengine:2025.1.1
- blackducksoftware/blackduck-redis:2025.1.1
- blackducksoftware/blackduck-registration:2025.1.1
- blackducksoftware/blackduck-scan:2025.1.1
- blackducksoftware/blackduck-storage:2025.1.1
- blackducksoftware/blackduck-webapp:2025.1.1

API enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

There are no new or changed API requests in 2025.1.1.

Binary scanner information

There are no updates to the binary scanner in Black Duck 2025.1.1.

For a comprehensive list of changes, see the Black Duck Binary Analysis release notes.

Fixed issues

The following customer-reported issues have been fixed in this release:

- (HUB-43061). Fixed an issue when using the `--detect.blackduck.signature.scanner.individual.file.matching=SOURCE` option could produce no results when scanning `.js` files.
- (HUB-43374). Added the missing description, source, and severity fields for the V8 `/api/projects/{projectId}/versions/{projectVersionId}/vulnerable-bom-components` endpoint.
- (HUB-43389, HUB-44090). Fixed an issue where security risks were still being counted in the BOM when the status of their vulnerabilities were set as Ignored/Mitigated/Remediation complete.
- (HUB-43931). Fixed an issue where components might not be consolidated in the project's Source tab.
- (HUB-44076). Fixed an issue where a blank page could be displayed when visiting https://HUB_URL/alert/ after updating Black Duck from version 2023.1.2 to 2024.4.1, and Alert from version 6.12.2 to 7.2.0.
- (HUB-44089). Fixed an issue where security vulnerabilities from removed components could still show up in the Security tab for a project.
- (HUB-44104). Fixed an issue where snippet matches continued to display with policy violations in the BOM and Source tab after being remediated as Confirmed and then marked as Ignore Match on the Source tab.
- (HUB-44185). Fixed a proxy issue that could cause the What's New window to be blank.
- (HUB-44186). Fixed database deadlock issues that could occur when updating `version_bom_risk_profile`.
- (HUB-44190). Fixed an issue where SPDX report generation could fail for projects with a CycloneDX SBOM mapped.
- (HUB-44210). Fixed an issue where expanding the Source tree in a BOM could result in a 400 Bad Request error.
- (HUB-44253). Fixed database deadlock issues that could occur when updating `version_bom_component`.
- (HUB-44365). Fixed an issue where a Duplicate key error could be generated when importing a CycloneDX SBOM that was merged using cyclonedx-cli tool into a single SBOM JSON file.
- (HUB-44366). Fixed an issue where the “scans” array was no longer included in the `aggregateBomViewEntries` array of the REST API doc for Version Report Endpoints.
- (HUB-44486). Fixed an issue where component matches in a Container scan were incorrectly stored when the same component identifier was present in both the base image layer and a custom layer.
- (HUB-44515). Migrated Detect Desktop to Black Duck, including download links and branding.
- (HUB-44549). Fixed an issue where Container Scans could generate different results after running apt update.
- (HUB-44584, HUB-44623). Fixed an issue where the `blackduck-postgres-init` job could fail in hosted environments, preventing the successful execution of the Create Hub job.

Black Duck SCA 2025.1.0

Announcements

New Gen05 sizing guidance

Black Duck has been upgraded to Gen05 sizing, offering significant improvements in resource optimization. The new hardware recommendations deliver 25% to 45% better efficiency, ensuring enhanced scalability and performance for modern workloads. Customers are encouraged to review the updated hardware requirements to take full advantage of these optimizations.

Detect 10 released and Detect 8 end of support

Detect 10 is now available, offering enhanced features and improvements. As part of this release, Detect 8 will reach end of support on October 31, 2024.

Key changes include:

- Customers with Detect 8.x already configured will see a red warning indicator upon upgrade, advising them to transition to a supported version. A warning will also be displayed if they attempte to change away from Detect 8.x, as this action is irreversible.
- The Detect 8.x option will no longer be available for new installations.
- For upgrades, Detect 8.x will only appear as an option for customers who previously had it configured.
- Detect 10 will now be the default for new customers or upgrades to version 2025.1.0 where the Detect property was previously unset.

Upcoming deprecation of project version hierarchical bill of materials

The project version hierarchical bill of materials (BOM) functionality in Black Duck is planned for deprecation in version 2025.4.0. Users relying on this functionality are encouraged to begin transitioning to alternative workflows to ensure uninterrupted processes.

New and changed features

New scan types available for SCA Scan Service (SCASS)

The SCA Scan Service (SCASS) has been enhanced to include support for Binary and Container scanning. This update expands the service's capabilities, enabling broader analysis and improved flexibility for users managing diverse scanning requirements.

New remediation statuses added

Black Duck now includes VEX (Vulnerability Exploitability eXchange) remediation status values, as described by the Cybersecurity and Infrastructure Security Agency (CISA). These values provide detailed tracking of the exploitability and remediation efforts for vulnerabilities, helping you assess and manage vulnerability risks more effectively. The following remediation status values have been added:

- Known Affected (AFFECTED): Actions are recommended to remediate or address this vulnerability.
- Known Not Affected (NOT AFFECTED): A justification must be provided to ensure that the decision is properly documented.
- Under Investigation (UNDER INVESTIGATION): It is not yet known whether these product versions are affected by the vulnerability. An update will be provided in a later release.

New feature to define default CPE for component versions

Black Duck now includes the ability to define a default Common Platform Enumeration (CPE) for component versions. This feature simplifies vulnerability tracking by ensuring that a consistent CPE is associated with each component version, reducing the need for manual updates. Users can configure a default CPE directly in the component version settings, steamlining SBOM generation and improving data accuracy.

New slide-out panel for BOM component information

In the Components tab for a project version, clicking a component now opens a slide-out panel instead of navigating to a new page. This update preserves the context of where the component is being used, eliminating the need to switch back and forth between pages for additional information.

New Exclude Unconfirmed Snippet Matches option added to SBOM Templates

A new SBOM template option, "Exclude Unconfirmed Snippet Matches" has been added to the Component Data section in SBOM templates. This option allows users to exclude components with unconfirmed snippet matches from their SBOM, providing a cleaner and more precise representation of the project's open source composition.

New scan CSV data

Black Duck now supports generating CSV data during scans using the new `--upload-csv` parameter in the scan CLI. This feature allows users to create a CSV file during the scan and automatically upload it to Black Duck. Additionally, users can download the CSV data directly from the Scans page and the project version's Settings tab in the Black Duck interface, providing flexible access to scan results for further analysis and reporting.

Added support for CycloneDX 1.6

You can now export the Software Bill of Materials report for your projects in CycloneDX v1.6 format. This can be done by viewing a project version, clicking the Reports tab, clicking the Create Report button, and then selecting CycloneDX v1.6 - JSON. For more information on CycloneDX v1.6, please visit the CycloneDX v1.6 reference page.

Added support for CVSS v4.x vulnerability score ranking

Black Duck now includes support for CVSS (Common Vulnerability Scoring System) version 4.0, providing enhanced granularity for Base metrics, a new Supplemental metric group, and an updated methodology for determining severity, among other improvements. For more details on CVSS v4.0, visit the official specification documentation at https://www.first.org/cvss/v4.0/specification-document.

Added support for SAML signed authentication certificates

Black Duck now supports SAML signed authentication certificates, enhancing security by validating authentication requests against a trusted certificate. System Administrators can manage certificates directly in the SAML configuration settings.

Updated JWT session token invalidation enabled by default

The feature to invalidate JWT session tokens upon logout is now enabled by default. This update enhances security by ensuring that session tokens are no longer valid after a user logs out.

Discontinued support for CVSS v2 vulnerability score ranking

CVSS v2 will no longer be supported as the highest-priority CVSS ranking. However, it will still be displayed if no CVSS v3.x or CVSS v4.x score exists for a vulnerability.

Container versions

- blackducksoftware/blackduck-postgres:15-1.10
- blackducksoftware/blackduck-postgres-upgrader:15-1.3
- blackducksoftware/blackduck-postgres-waiter:1.0.14
- blackducksoftware/blackduck-cfssl:1.0.30
- blackducksoftware/blackduck-nginx:2025.1.0
- blackducksoftware/blackduck-logstash:1.0.40
- blackducksoftware/bdba-worker:2024.12.2
- blackducksoftware/rabbitmq:1.2.42
- blackducksoftware/blackduck-authentication:2025.1.0
- blackducksoftware/blackduck-bomengine:2025.1.0
- blackducksoftware/blackduck-documentation:2025.1.0
- blackducksoftware/blackduck-integration:2025.1.0
- blackducksoftware/blackduck-jobrunner:2025.1.0
- blackducksoftware/blackduck-matchengine:2025.1.0
- blackducksoftware/blackduck-redis:2025.1.0
- blackducksoftware/blackduck-registration:2025.1.0
- blackducksoftware/blackduck-scan:2025.1.0
- blackducksoftware/blackduck-storage:2025.1.0
- blackducksoftware/blackduck-webapp:2025.1.0

API enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Removed support for `access_token` request parameter

Support for passing the authorization token (JWT) as a request parameter via the access_token request have been removed to address a security vulnerability. Users should ensure authorization tokens are passed using the Authorization HTTP header as documented in the REST API developer's guide.

Binary scanner information

The binary scanner has been updated to version **2024.12.2**.

Release highlights

- Added support for ARM64 architecture
- NET scanner updated:

- Reduced unknown version components on BOM for less manual triage
- More accurately reflect .NET component structure

For a comprehensive list of changes, see the Black Duck Binary Analysis release notes.

Fixed issues

The following customer-reported issues have been fixed in this release:

- (HUB-39655). Fixed an issue in Kubernetes deployments where the Black Duck webapp can enter a crash loop when the logstash disk is filled due to high activity. To address this, a log deletion script has been implemented to manage logstash disk usage.
- (HUB-42725). Fixed an issue where pagination label on the Notification page may not display the actual amount of notifications on the page.
- (HUB-43212). Fixed an issue where changes to the `maxRamPercentage` setting were only applied with Gen04 sizing, causing issues for hosted customers using Gen02 sizing.
- (HUB-43295). Fixed an issue on the Find page → Vulnerability tab where the "used by " section could display the wrong project version.
- (HUB-43394). Fixed an issue where the UI displayed "Conditionally Approved" instead of "Limited Approval" for policy conditions related to license statuses. The terms are now consistent across the platform.
- (HUB-43426). Fixed an issue where partition logs could overlap each other.
- (HUB-43431). Added increased error tolerance to the `upload-cache-source-migrator.pl` script to log failures but allow the process to continue.
- (HUB-43556). Fixed an issue where the project versions comparison view could display no results after changing the filter from "Total Changed" to "New Components".
- (HUB-43560). Fixed an issue where a user with the Project Creator role, designated as the manager of an individual project group, was able to move any project between groups. These users are now correctly restricted moving only the projects they have created.
- (HUB-43791). Fixed an issue where the `PUT /api/projects/{projectId}` endpoint required a `projectOwner` parameter/value to be present despite it only requiring the `name` parameter for the project.
- (HUB-43826). Fixed an issue with the `GET /api/projects/{projectId}/versions/{projectVersionId}/reports/{reportId}/contents` endpoint where the error message displayed describing the maximum limit on file size indicated that it applied only to HTML reports. The message now also includes JSON streams.
- (HUB-43839). Fixed an issue where the unconfirmed snippets policy did not return results using the priority tag under the Find page.
- (HUB-43841). Fixed an issue where adding a license to a project version under Settings → Version Details Tab and then generating an SBOM Report, the Extracted Text could display as NONE.
- (HUB-43847). Fixed an issue where special characters in the component name could cause the security tab to return zero vulnerability results.
- (HUB-44004). Fixed an issue where updating a subproject with version to subproject with unknown version could generate an error in the BOM.

- (HUB-44114). Fixed an issue where the `/api/projects/{projectId}/versions/{projectVersionId}/components` endpoint was allowing the addition of a project to a BOM without a version.
- (HUB-44184). Fixed an issue in the component bulk edit window when the number of selected items was displayed, it displayed “{count}” instead of actual numbers in the Japanese localization of Black Duck.

Black Duck SCA 2024.10.x

Black Duck 2024.10.1

Announcements

Added support for ARM64 architecture

Black Duck now includes support for ARM64 architecture, expanding compatibility to a broader range of systems and environments. ARM64 (also known as AArch64) is widely used in modern server platforms, including ARM-based cloud environments like AWS Graviton, as well as in embedded and IoT devices. This update ensures that users running ARM64-based systems can leverage Black Duck's capabilities for open source risk management effectively.

Please note, as of 2024.10.1, BDBA and RL-service are not supported on ARM systems. Support for BDBA support is planned for version 2025.1.0, while RL-service support is not planned at this time.

New and changed features

New SCA Scan Service for Package Manager and Signature Scans

Black Duck now offers the SCA Scan Service (SCASS), a scalable solution for performing software composition analysis scans outside of the traditional Black Duck SCA environment. SCASS supports Package Manager and Signature Scans, making it a versatile choice for various scanning needs.

This services provides significant benefits for both on-premise and hosted customers:

- On-premise customers: Resource requirements for non-specialized scanning are greatly reduced, steamlining infrastructure needs.
- Hosted customers: Cloud Infrastructure efficiency improves with dynamic scaling based on overall scan demand, enhancing performance and reducing operational overhead.

SCASS also enables Correlated Scanning, a new feature that leverages SCASS to enhance match results by combining insights from multiple scanning techniques.

Additionally, SCASS delivers faster delivery of scanning bug fixes, independent of Black Duck release cycles. While scan results are stored transactionally, this streamlined service enhances the flexibility and scalability of scanning across platforms.

Please note, this feature must be enabled on your product registration key to take advantage of the service. With SCASS, you can simplify resource management and enjoy a more scalable scanning experience. Contact your Black Duck representative to learn more.

New sorting feature in LTS vulnerability view

The LTS vulnerability view now includes sorting capabilities, allowing you to organize vulnerabilities by the following criteria for improved navigation and analysis:

- Vulnerability ID (default)
- Affected Components, the first component in the list
- Overall Score
- Remediation Status

New URL field added to Project Settings page

A new URL field has been added to the Project Settings page to define the homepage value in an SBOM when a project version is used as a component in a parent project.

- The URL field is used as the Homepage in an SBOM if enabled in the template.
- The field is empty for new projects unless cloned from one with a pre-populated URL.
- The same URL applies to all project versions; it cannot be overridden at the BOM Component level.

Match confidence for package manager matches removed from BOM

Match confidence scores for package manager matches are no longer included in the Bill of Materials (BOM). This update reflects the inherent accuracy of package manager matches, where ambiguity is unlikely. Match confidence continues to be applied for other types of component matches.

Merged Kubernetes and Openshift install guides

The previously separate installation guides for Kubernetes and Openshift have been merged into a single, unified guide. This streamlined documentation simplifies the installation process by consolidating all relevant instructions in one place. Please note that the Swarm install guide is still maintained as a separate document.

Updated maximum upload size change for binary and container scans

Starting in Black Duck 2024.10.0, customers can now increase the maximum upload size for binary and container scans from the default of 5 GB to 100 GB by adjusting the `BINARY_UPLOAD_MAX_SIZE` environment variable. The documentation has been updated to reflect this new configuration change.

Container versions

- blackducksoftware/blackduck-postgres:15-1.8
- blackducksoftware/blackduck-postgres-upgrader:15-1.1
- blackducksoftware/blackduck-postgres-waiter:1.0.14
- blackducksoftware/blackduck-cfssl:1.0.30
- blackducksoftware/blackduck-nginx:2024.10.1
- blackducksoftware/blackduck-logstash:1.0.39
- blackducksoftware/bdba-worker:2024.9.1
- blackducksoftware/rabbitmq:1.2.41
- blackducksoftware/blackduck-authentication:2024.10.1
- blackducksoftware/blackduck-bomengine:2024.10.1
- blackducksoftware/blackduck-documentation:2024.10.1
- blackducksoftware/blackduck-integration:2024.10.1

- blackducksoftware/blackduck-jobrunner:2024.10.1
- blackducksoftware/blackduck-matchengine:2024.10.1
- blackducksoftware/blackduck-redis:2024.10.1
- blackducksoftware/blackduck-registration:2024.10.1
- blackducksoftware/blackduck-scan:2024.10.1
- blackducksoftware/blackduck-storage:2024.10.1
- blackducksoftware/blackduck-webapp:2024.10.1

API enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Added sorting to LTS vulnerability view endpoint

The `GET /api/lts-projects/{projectId}/lts-project-versions/{versionId}/vulnerabilities` API endpoint now supports sorting on the following points:

- Vulnerability ID (default)
- Affected Components, the first component in the list
- Overall Score
- Remediation Status

Binary scanner information

The binary scanner has been updated to version 2024.9.1. For more information on this release, please see the Black Duck Binary Analysis release notes.

Fixed issues

The following customer-reported issues have been fixed in this release:

- (HUB-43265). Fixed an issue where cloning projects with users and groups selected and there are no user groups assigned to the project could generate a HTTP 400 - Parameter set is empty stack trace error.
- (HUB-43391). Fixed an issue where ignored components/subprojects could still be included in SBOM reports.
- (HUB-43413). Fixed an issue where components with no comments could sometimes appear when "components with comments" filter is set.
- (HUB-43588). Fixed an issue where the License Risk count at the top of the Component page did not update promptly after a component's license was changed, sometimes taking several days to reflect the change.
- (HUB-43760). Fixed an issue where the string "(c) Copyright" could cause the copyright normalization job to fail.
- (HUB-43860). Fixed an issue where database dumps of `bds_hub` could fail to restore due to a mismatch in view definitions.

Black Duck SCA 2024.10.0

Announcements

Black Duck SCA is now part of Black Duck, a fully independent entity from Synopsys

With this update, you will notice branding changes, including the new Black Duck logo. For more information please see Black Duck takes flight.

Additionally, we have launched a new website and community portals. Please update any Black Duck documentation and bookmarks you have saved. For details on the new URLs please see Black Duck Domain Change FAQ.

As part of this process, sig-repo.synopsys.com is being phased out. Please switch to using repo.blackduck.com. We recommend keeping sig-repo.synopsys.com on your allow list until February 2025, when it will be completely replaced by repo.blackduck.com.

Introducing ceiling-based rate limiting policies

Starting in Q1 2025, we will begin rolling out ceiling-based rate limiting policies. This change is expected to have minimal impact initially, and will likely be introduced first for Black Duck Hosted customers.

- Black Duck will be closely monitoring this rollout and will take necessary actions for customers that do hit the ceiling threshold.
- Customers with high API traffic load may experience rate limiting under heavy usage scenarios. If you encounter `HTTP 429 - Too Many Requests` responses, we strongly recommend implementing a strategy to reduce API traffic when building custom API integration applications.

Java Development Kit (JDK) upgraded to version 17

Black Duck 2024.10.0 has been updated to use JDK 17, upgrading from JDK 11. This upgrade brings enhanced performance, improved security, and long-term support, ensuring a more robust and future-ready environment for both the hosted and on-prem products.

Users and developers working with both versions should ensure their environments are compatible with JDK 17 to take full advantage of this update.

Upcoming deprecation of BDIO1

Please note that the BDIO1 format of BDIO files will be deprecated starting with the 2025.1.0 release. Detect version 8 and later utilize BDIO2+, while only unsupported versions of Detect continue to use BDIO1.

BDIO (Black Duck I/O) files are JSON-based files that store scan results, including open source components, dependencies, vulnerabilities, and licenses in a project. They enable efficient data transfer between Black Duck scanners and the platform for further analysis and integration into development workflows.

For customers running earlier versions of Black Duck that still use BDIO1, we will continue to support it in those versions. If you modify BDIO1 files, these modifications will remain compatible with Black Duck versions 2024.10.0 or earlier. However, when upgrading to Black Duck version 2025.1.0 or later, you will need to update your modifications to work with BDIO2, BDIO3, or newer versions.

There are no changes to BDIO2 and BDIO3 support; both will continue to be fully supported.

End of support for PostgreSQL 14

With the 2024.10.0 release, Black Duck drops support for external PostgreSQL 14. Please refer to the PostgreSQL Version Upgrade Schedule page for more information.

Upgrade restrictions for PostgreSQL container users

For users of the Black Duck-provided PostgreSQL container, Black Duck 2024.10.0 only supports direct upgrades from earlier versions of Black Duck that use the PostgreSQL 13 or 14 containers (2022.10.0 to 2024.7.x inclusive).

Upgrading from older Black Duck versions (prior to 2022.10.0) will require a 2-step upgrade:

1. Upgrade to Black Duck 2023.7.x.
2. Upgrade to Black Duck 2024.10.x.

PostgreSQL container migration to version 15

Black Duck migrates its PostgreSQL image to version 15 with the 2024.10.0 release. Customers not using the Black Duck-supplied PostgreSQL image are not affected.

Regarding binary scanning performance metrics

This guidance offered on the Black Duck Hardware Scaling Guidelines is valid when binary scans are 20% or less of the total scan volume (by count of scans). The performance testing metrics should be used as guideline for scaling the server. Not all binaries that are of a certain size are the same in that the number of layers of extraction and the number of identified components found within the binary can require more or less resources than what was determined in the performance tests.

New and changed features

New Multi-Factor Authentication (MFA) feature

Black Duck 2024.10.0 now includes a new Multi-Factor Authentication (MFA) feature, providing enhanced security for user accounts. With MFA enabled, users will authenticate using a MFA token, SMS or app based verification code for the second layer of verification. This additional step helps ensure that only authorized users can access the system, further safeguarding sensitive data.

New Correlated scanning

A new scanning method has been added to Black Duck 2024.10.0 which correlates match results from Package Manager and Signature scans to enhance results. By integrating the strengths and compensating for the weaknesses of different scanning methods, Correlated Scanning effectively reduces false positives and version spray. The correlation between these scanning methods ensures more accurate and comprehensives results.

Black Duck 2024.10.0 supports correlation between single signature scans and one/many package manager scan results only. Using it with other scan types is not recommended.

New Origin IDs tab added to Component version page

A new Origin IDs tab has been added to the Component version page. This tab lists all known external IDs and Package URLs (PURLs) associated with a specific component version, providing more detailed visibility into the origins of each component.

New file adjustment simplification

The file adjustment process has been simplified to use path-based adjustments instead of signature-based adjustments. This change improves user experience, enhances performance, and removes obstacles to advancing signature-based component matching in the KnowledgeBase. For example, if the same file, directory, or archive appears in multiple locations (e.g., in different code locations mapped to the same project version), only one instance will be adjusted.

New session token invalidation after logout

This new feature allows session token to be invalidated after a user logs out of the system. This enhances security by ensuring that tokens cannot be reused after logout. However, this feature is not enabled by default. To activate it, administrators must configure the `blackduck-config.env` file and set the `JWT_BLOCK_LIST_CHECK` variable to `true`.

Updated external authentication configuration location

The external authentication configuration pages for SAML and LDAP have been moved from Admin → System Settings → User Authentication to Admin → Integrations → External Authentication.

In addition, the User Authentication page has been renamed to Local Authentication to reflect its updated functionality.

Updated support for multiple container scans to a single project version

We have enhanced the system to allow multiple container scans to be mapped to a single project version. Previously, only one container scan could be mapped per project version. This enhancement provides greater flexibility in managing and analyzing your codebase across different containers. The following are valid combinations of scans (code locations) that can be mapped to single project version:

- Any combination of non-container scans mapped to project version.
- One or many container scans mapped to project version.
- One or many container scans along with one or many IaC/Malware scans mapped to the same project version.

All other combinations of mapped code locations are invalid and the scan process will fail if the mapping of corresponding code location will result in invalid combination.

As part of this update, a migration will be required to change how container names are constructed. Previously, container names were derived from their code location. Moving forward, they will be generated from the URI of the container tar file, as provided in the BDIO file.

Added vulnerability remediation for LTS projects

Long-term support (LTS) projects now support setting the remediation status for vulnerabilities, helping teams track and document the resolution process for vulnerabilities within their projects.

Updated rate limiting configuration

Rate limiting has been disabled by default in Black Duck to enhance overall system performance. If needed, rate limiting can still be manually re-enabled by setting the `BLACKDUCK_USE_HEAP_RATE_LIMITING` environment variable to `ON`.

Minimum supported browser versions

- Safari Version 16.1

- Chrome Version 107 (x86_64)
- Firefox Version 106 (64-bit)
- Microsoft Edge Version 107 (64-bit)

Container versions

- blackducksoftware/blackduck-postgres:15-1.8
- blackducksoftware/blackduck-postgres-upgrader:15-1.1
- blackducksoftware/blackduck-postgres-waiter:1.0.14
- blackducksoftware/blackduck-cfssl:1.0.30
- blackducksoftware/blackduck-nginx:2024.10.0
- blackducksoftware/blackduck-logstash:1.0.39
- blackducksoftware/bdba-worker:2024.9.1
- blackducksoftware/rabbitmq:1.2.41
- blackducksoftware/blackduck-authentication:2024.10.0
- blackducksoftware/blackduck-bomengine:2024.10.0
- blackducksoftware/blackduck-documentation:2024.10.0
- blackducksoftware/blackduck-integration:2024.10.0
- blackducksoftware/blackduck-jobrunner:2024.10.0
- blackducksoftware/blackduck-matchengine:2024.10.0
- blackducksoftware/blackduck-redis:2024.10.0
- blackducksoftware/blackduck-registration:2024.10.0
- blackducksoftware/blackduck-scan:2024.10.0
- blackducksoftware/blackduck-storage:2024.10.0
- blackducksoftware/blackduck-webapp:2024.10.0

API enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

New and updated endpoints for Multi-Factor Authentication (MFA)

As part of the new Multi-Factor Authentication (MFA) feature, the following new API endpoints have been introduced:

- **Get Current User MFA Secret**

  `GET /api/current-user/mfa`

- **Setup MFA for current user**

  `POST /api/current-user/mfa`

- **Reset MFA for current user**

  `DELETE /api/current-user/mfa`

- **Reset MFA for user**

  `DELETE /api/users/{userId}/reset-mfa`

- **Authenticate MFA for current user**

  `POST /api/mfa/authenticate`

In addition, the responses for the following endpoints have been updated to include information on whether each user has Multi-Factor Authentication (MFA) set up.

- **Listing Users**

  `GET /api/users`

- **Reading the Current User**

  `GET /api/current-user`

Updated `users` and `current-user` endpoints

The `GET /api/users` and `GET /api/current-user` endpoint response has been updated to include information on whether each user has Multi-Factor Authentication (MFA) set up.

New endpoints for container multi-part uploads

New API endpoints have been introduced to enhance the file upload process with container multi-part uploads. These endpoints allows you to upload large files in smaller chunks, improving efficiency and reliability. The new endpoints are:

- **Start Upload**

  `POST /api/storage/containers/{container_id}/multipart`

- **Upload Part of File**

  `PUT /api/storage/containers/{container_id}/multipart`

- **Finish Upload Request**

  `POST /api/storage/containers/{container_id}/multipart/completed`

- **Cancel Upload Request**

  `DELETE /api/storage/containers/{container_id}/multipart`

For detailed usage and payload instructions, please refer to the REST API Developers Guide available in Black Duck.

SBOM fields API discontinuation notice

As of Black Duck 2024.10.0, the following three sbom-fields APIs have been discontinued and will return a `410 GONE` response with no content:

- **Listing SBOM Field Scopes**

  `GET /api/sbom-fields/scopes`

- **Listing SBOM Fields In Scope**

  `GET /api/sbom-fields/scopes/{scopeName}/fields`

- **Updating a SBOM Field's Status**

  `PUT /api/sbom-fields/scopes/{scopeName}/fields/{fieldId}`

These APIs have also been removed from the REST API Developer's Guide, and will be fully removed in an upcoming release.

Deprecated LTS API endpoints

The following LTS API endpoints have been deprecated and will be removed in an upcoming release:

- **Updating a LTS Project by projectId**

  `PUT /api/lts-projects/{projectId}`

  LTS projects can be updated with the `PUT /api/projects/{projectId}` endpoint.

- **Deleting a LTS Project by projectId**

  `DELETE /api/lts-projects/{projectId}`

  LTS projects can be deleted with the `DELETE /api/projects/{projectId}` endpoint.

- **Updating a LTS Project Version**

  `PUT /api/lts-projects/{projectId}/lts-project-versions/{projectVersionId}`

  LTS project version information can be updated with the `PUT /api/projects/{projectId}/versions/{projectVersionId}` endpoint.

Added HATEOAS links to API endpoints

The following endpoints have been updated to include HATEOAS links in their responses. These links provide dynamic navigation and allow clients to discover available actions or related resources without needing to hardcoded URLs.

- **Updating a Project Version's BOM State**

  `PUT /api/projects/{projectId}/versions/{projectVersionId}/transition`

- **Reading LTS Projects**

  `GET /api/lts-projects`

- **Reading a LTS Project by projectId**

  `GET /api/lts-projects/{projectId}`

- **Updating a LTS Project by projectId**

  `PUT /api/lts-projects/{projectId}` (DEPRECATED)

- **Deleting a LTS Project by projectId**

  `DELETE /api/lts-projects/{projectId}` (DEPRECATED)

Although two of these endpoints are deprecated, they have also received HATEOAS links as part of the update to the non-deprecated endpoints. While this update was intended primarily for the active endpoints, the deprecated ones were impacted due to shared response formatting.

Binary scanner information

The binary scanner has been updated to version 2024.9.1. For more information on this release, please see the Black Duck Binary Analysis release notes.

Fixed issues

The following customer-reported issues have been fixed in this release:

- (HUB-33532). Fixed an issue in the Version Details report where an improperly escaped backslash character could cause an invalid JSON format error when viewing the report content.
- (HUB-36358). Fixed an issue where the Signature Scanner could fail when scanning files compressed using the Pack200 format. This issue occurred due to an incompatibility introduced by a new version of the Apache Commons Compress library. The problem has been resolved with a local update to this library.
- (HUB-41944). Fixed an issue when modifying a custom field for a specific component version, the "Updated" field in the component details tab did not reflect the change but the changes to the component version details and license are reflected correctly.
- (HUB-42604). Fixed an issue where the match count shown on the Components page of the BOM was displaying a different count from the Source page.
- (HUB-43043). Fixed an issue where the BOM page would automatically refresh after reviewing/unreviewing a component, changing a component's version/license, ignoring/unignoring a component, manually adding a component, adding a comment, confirming/editing/ignoring a snippet match. The table now still refreshes, but in the background no longer disappears.
- (HUB-43170). Fixed an issue where a Signature Scan could produce a `java.nio.file.InvalidPathException` warning message in cli output when invalid archive file encountered.
- (HUB-43220). Optimized a query used in license API endpoints (`/api/internal/composite/licenses/{licenseId}/usages` and `/api/licenses/{licenseId}/bom-counts`) which was causing longer than expected load times.
- (HUB-43307). Updated the OpenJDK version to Zulu Java 17.0.12 in Black Duck to address vulnerability issues.
- (HUB-43315). Fixed a performance issue related to the query to extract the copyrights in report generation post upgrade Black Duck 2024.7.0.
- (HUB-43342). Fixed an issue where notes added to a license were not displaying in the BOM License Details. We will show them under a Notes section from of collapsible element with a show more/show less button in case notes are long. If the license does not have any notes added, the Notes section will not appear.
- (HUB-43382). Fixed an issue where source file adjustments for binary scans could affect mutliple files where matches are shown for both a binary and within a JAR file. Source file adjustments for binary scans are now disabled.
- (HUB-43389). Fixed an issue where risk warning data was not being retained after unmapping the scan and then remapping.
- (HUB-43502). Created a new index on the `version_bom_applied_adjustment` table to improve performance when updating license texts.

Black Duck SCA 2024.7.x

Black Duck 2024.7.3

Announcements

Black Duck SCA is now part of Black Duck, a fully independent entity from Synopsys

With this update, you will notice branding changes, including the new Black Duck logo. For more information please see Black Duck takes flight.

Additionally, we have launched a new website and community portals. Please update any Black Duck documentation and bookmarks you have saved. For details on the new URLs please see Black Duck Domain Change FAQ.

As part of this process, sig-repo.synopsys.com is being phased out. Please switch to using repo.blackduck.com. We recommend keeping sig-repo.synopsys.com on your allow list until February 2025, when it will be completely replaced by repo.blackduck.com.

New and changed features

There are no new or changed features in Black Duck 2024.7.3.

Container versions

- 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:2024.7.3
- blackducksoftware/blackduck-logstash:1.0.38
- blackducksoftware/bdba-worker:2024.6.3
- blackducksoftware/rabbitmq:1.2.40
- blackducksoftware/blackduck-authentication:2024.7.3
- blackducksoftware/blackduck-bomengine:2024.7.3
- blackducksoftware/blackduck-documentation:2024.7.3
- blackducksoftware/blackduck-integration:2024.7.3
- blackducksoftware/blackduck-jobrunner:2024.7.3
- blackducksoftware/blackduck-matchengine:2024.7.3
- blackducksoftware/blackduck-redis:2024.7.3
- blackducksoftware/blackduck-registration:2024.7.3
- blackducksoftware/blackduck-scan:2024.7.3
- blackducksoftware/blackduck-storage:2024.7.3
- blackducksoftware/blackduck-webapp:2024.7.3

API enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

There are no new or changed API endpoints in Black Duck 2024.7.3.

Binary scanner information

The binary scanner has been updated to version 2024.6.3. For more information on this release, please see the Black Duck Binary Analysis release notes.

Fixed issues

There are no customer-reported bugs fixed in this release.

Black Duck SCA 2024.7.2

Announcements

There are no new announcements for Black Duck 2024.7.2.

New and changed features

New secure JWT key pair provisioning

We have enhanced our JWT handling by allowing the secure provisioning of public/private key pairs, improving overall security and operational efficiency. This provisioning is optional and not a requirement for deployment. Instead of automatically generating and storing these key pairs in the database, you can now securely provide them to the services that require them.

Currently, only RSA keys (PEM encoded) are supported. Specifically, public keys must be in X.509 format, and private keys must be in PKCS#8 format. The private key is primarily needed by services that issue JWTs, such as the Authentication service, while the public key is required by any service offering public APIs that require authorized access.

Container versions

- 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:2024.7.2
- blackducksoftware/blackduck-logstash:1.0.38
- blackducksoftware/bdba-worker:2024.6.3
- blackducksoftware/rabbitmq:1.2.40
- blackducksoftware/blackduck-authentication:2024.7.2
- blackducksoftware/blackduck-bomengine:2024.7.2
- blackducksoftware/blackduck-documentation:2024.7.2
- blackducksoftware/blackduck-integration:2024.7.2

- blackducksoftware/blackduck-jobrunner:2024.7.2
- blackducksoftware/blackduck-matchengine:2024.7.2
- blackducksoftware/blackduck-redis:2024.7.2
- blackducksoftware/blackduck-registration:2024.7.2
- blackducksoftware/blackduck-scan:2024.7.2
- blackducksoftware/blackduck-storage:2024.7.2
- blackducksoftware/blackduck-webapp:2024.7.2

API enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Updated snippet matching API

The `POST /api/snippet-matching` API request has been updated to accept fingerprints generated from source code via an algorithm provided by Black Duck to customers.

Binary scanner information

The binary scanner has been updated to version 2024.6.3.

Fixed issues

There are no customer-reported bugs fixed in this release.

Black Duck SCA 2024.7.1

Announcements

There are no new announcements for Black Duck 2024.7.1.

New and changed features

Updated Component Origin Copyright Dialog

Currently, we show the `kbCopyright` text in the Component Origin Copyright dialog box, but only if the copyright was modified. With this update, we now always show the full copyright text in a second text block below the existing block with the label “Full Copyright Text” for reference. This information is not editable.

Enhanced dashboard with LTS version indicator

The dashboard has been enhanced to include an indicator for projects that have a Long-Term Support (LTS) version. Users can now more easily identify which projects have LTS project versions directly from the dashboard, improving visibility and management for long-term support projects.

Enhanced BOM Components tab with External IDs

The BOM Components tab will now utilize the new `inputExternalIds` field to provide more useful information for BINARY and CONTAINER matches. The current message has been updated and will be displayed when the following conditions are present on the component:

- `matchTypes` includes BINARY.

- `componentVersion` is missing in the response for the component.
- `origins` is empty in the response for the component.

The current message with the update is as follows (updated section in italics):

> **Unknown Version**
>
> This component has an unknown version. The license risks are estimated. For a more accurate result, manually specify a version for the component.
>
> *This identifier was found during binary scanning:*
>
> *<Data>*
>
> OR
>
> *These identifiers were found during binary scanning:*
>
> *<Data>*
>
> *<Data>*

For users utilizing the APIs, the `inputExternalIds` field is always available for supported scans. While not present in all scan types, they will appear for all BOM items in scans that utilize this feature.

Container versions

- 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:2024.7.1
- blackducksoftware/blackduck-logstash:1.0.38
- blackducksoftware/bdba-worker:2024.6.3
- blackducksoftware/rabbitmq:1.2.40
- blackducksoftware/blackduck-authentication:2024.7.1
- blackducksoftware/blackduck-bomengine:2024.7.1
- blackducksoftware/blackduck-documentation:2024.7.1
- blackducksoftware/blackduck-integration:2024.7.1
- blackducksoftware/blackduck-jobrunner:2024.7.1
- blackducksoftware/blackduck-matchengine:2024.7.1
- blackducksoftware/blackduck-redis:2024.7.1
- blackducksoftware/blackduck-registration:2024.7.1
- blackducksoftware/blackduck-scan:2024.7.1
- blackducksoftware/blackduck-storage:2024.7.1
- blackducksoftware/blackduck-webapp:2024.7.1

API enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

New `ltsReleaseCount` property for risk-profile-dashboard request

A new property has been added to the `GET /api/risk-profile-dashboard` API request. The `ltsReleaseCount` property returns the number of versions that are converted to LTS.

Updated /api/versions/{projectVersionId}/license-reports (POST)

The categories LICENSE_TEXT and LICENSE_DATA are no longer added to all notices reports. If the request includes no categories, it will default to LICENSE_TEXT and LICENSE_DATA. If the request includes DEEP_LICENSE_DATA or FILE_LICENSE_DATA, LICENSE_TEXT and LICENSE_DATA is added to the request. In all other cases, the report will only include the categories in the API request.

Updated vulnerable-bom-components API request

A new, optional `showUnscoredRelatedVulnerability` request parameter has been added to the `GET /api/projects/{projectId}/versions/{projectVersionId}/vulnerable-bom-components` API request. This parameter accepts a true/false value to include or exclude unscored related vulnerabilities in the response for the vulnerable-bom-components API.

If the parameter is not included or is set to false, the API response will remain consistent with the existing behavior. When set to true BDSAs will always list related CVEs, even if the affect component version ranges differ between the BDSA and CVE. This is to aid customers who use the CVE ID as a part of downstream vulnerability processes.

API deprecation notice

As of Black Duck 2024.7.1, the following three APIs have been marked as deprecated and will be removed in an upcoming release:

- `GET /api/sbom-fields/scopes`
- `GET /api/sbom-fields/scopes/{scopeName}/fields`
- `PUT /api/sbom-fields/scopes/{scopeName}/fields/{fieldId}`

Binary scanner information

The binary scanner has been updated to version 2024.6.3.

Fixed issues

The following customer-reported issues have been fixed in this release:

- (HUB-42054). Fixed an issue with the `/api/projects/{projectId}/versions/{projectVersionId}/risk-profile` API request returning unknown security risk for ignored confirmed snippets match types on components tab.
- (HUB-42392). Fixed an issue where an `ERR05_1028` exception error could occur when old, unmapped Scans were being purged.
- (HUB-42549). Fixed an issue where a `LicenseConflictBaseStrategy` warning was appearing repeatedly during BOM computation.
- (HUB-42626). Added a workaround for an issue where, under certain situations where a DNS server is configured, a bug in the curl/c-ares package (included in all alpine based images) prevented resolution

of the cfssl domain, which caused the containers to crash because they weren't able to obtain the necessary certificates to deploy.

NOTE: The maintainer of c-ares has release a patch for this bug. However, it is not yet available in a stable release of Alpine Linux, and the availability timeline is currently uncertain.

- (HUB-42786). Fixed a snippet match query optimisation issue where project versions with a large number of unconfirmed snippet matches could cause the BOM component page to load more slowly.
- (HUB-42811). Fixed an API pagination issue with the `vulnerable-bom-components` endpoint which could affect projects with large amount of vulnerabilities (500+).
- (HUB-42922). Fixed an issue where modifying the remediation status could fail on the Vulnerability Affected Projects page, displaying a "Cannot read properties of undefined (reading 'protocol')" error in the Update Remediation Plan dialog.
- (HUB-42939). Fixed an issue where IdP metadata was not being refreshed. Black Duck will now reload the configuration for SAML every half hour, which includes the IdP metadata.
- (HUB-43029). Fixed an issue where running the webapp with a non standard set of user and group could cause the logfiles to not be available on the UI due to an error generating the zip file.
- (HUB-43052). Fixed a sorting issue on the Scans page where sorting the "Updated" column multiple times and then sorting by another column, navigating away and returning to the page without refreshing could result in the page not retaining the "Updated" sort order.
- (HUB-43060). Fixed an issue where custom field details were not wrapped on the Settings page despite line breaks being set.
- (HUB-43257). Fixed an issue where the content displayed in the What's New window would not render if the browser local was set to an unsupported language.
- (HUB-43258). Fixed an issue where the Component policy status and Overridden By columns of the Version details report were empty in source.csv report.
- (HUB-43378). Fixed an issue where the `--detect.code.location.name` parameter was not working with BDBA scans.

Black Duck SCA 2024.7.0

Announcements

KnowledgeBase upgrade post upgrade

Please be aware that a KnowledgeBase update job will run upon completion of Black Duck upgrade. This update addresses outdated KnowledgeBase component license data resulting from a previous bug. Depending on the size of your deployment, the job may take up to 4 hours to complete, though typical durations are shorter. This process will not impact scans or other Black Duck processes. However, during the execution of this job, you may observe increased CPU and memory usage in the Job runner pods.

Updated Activity Audit Trail

The Activity Audit Trail feature allows for the retention of activity audit records of user actions and key events, such as project version component and vulnerability records, in the application affecting a project and/or project version.

With this update, the functionality can now be disabled to improve performance and decrease storage costs, giving you greater flexibility and control over your project's audit records. When Activity Audit Trail is disabled, activity data is not tracked. Re-enabling it will start tracking activity from that moment on.

This feature is disabled by default for fresh installations but remains enabled for existing installations and upgrades.

PostgreSQL 16 support for external databases

Black Duck now supports and recommends PostgreSQL 16 for new installs that use external PostgreSQL. However, Google CloudSQL for PostgreSQL does not yet support PostgreSQL 16; on that platform, Black Duck recommends PostgreSQL 15.

Migrating to 2024.7.x does not require migration to PostgreSQL 16.

No action is required for users of the internal PostgreSQL container.

Upcoming end of support for PostgreSQL 14

With the upcoming 2024.10.0 release, Black Duck will end support for external PostgreSQL 14. Please refer to the Black Duck 2023.10.0. Please refer to the PostgreSQL Upgrade Schedule page for more information.

Upcoming PostgreSQL container migration to version 15

Black Duck will migrate its PostgreSQL image to version 15 with the 2024.10.0 release. Customers not using the Black Duck-supplied PostgreSQL image will not be affected.

Upcoming upgrade restrictions for PostgreSQL container users

For users of the Black Duck-provided PostgreSQL container, Black Duck 2024.10.0 will only support direct upgrades from earlier versions of Black Duck that use the PostgreSQL versions 13 or PG 14 containers (2022.10.0 to 2024.7.x inclusive).

Upgrading from older Black Duck versions (prior to 2022.10.0) will require a 2-step upgrade:

1. Upgrade to Black Duck 2023.7.x.
2. Upgrade to Black Duck 2024.10.x.

Upcoming webserver technology replacement

In an upcoming Black Duck release (2024.10.0 or 2025.1.0), the existing ingress webserver (NGiNX) will be replaced with a new technology, Apache APISIX. Customers with existing custom NGiNX configuration will need to update their settings to ensure compatibility.

Documentation localization

The 2024.4.0 version of the UI, online help, and release notes have been localized to Japanese and Simplified Chinese.

Starting with 2024.7.0, updated Japanese and Simplified Chinese localizations of the documentation will be posted on the Black Duck Documentation Portal immediately when available.

New and changed features

What's New window

Discover the latest features and enhancements introduced in the current Black Duck release with the new What's New window. After an upgrade, the What's New window will appear upon login, highlighting the most impactful updates in this version.

Users can choose to disable this window for future logins, but it will reappear with the next Black Duck server upgrade. Even after being dismissed, the What's New content can be accessed under the Help menu. All major versions of Black Duck from 2024.7 onward will include What's New content.

New Long-Term Support (LTS) feature

Long-Term Support (LTS) project versions enable tracking of vulnerability data for released product versions. LTS projects are intended for software already in use by end users or customers. Designed with scalability in mind, LTS projects can support extremely high volumes of project versions.

LTS project versions retain minimal data from Active project versions, focusing on tracking newly discovered vulnerabilities in the components within the LTS Bill of Materials (BOM). When converting an Active version to LTS, a Software Bill of Materials (SBOM) is automatically created to facilitate sharing with required third parties. While LTS version do not currently support notifications, they will receive new vulnerability data as it is published to the Black Duck KnowledgeBase.

New BDSA AI Assisted tag

A new mechanism has been introduced to automate the creation of BDSAs using AI models and have introduced an “AI Assisted” BDSA tag. AI Assisted Security Advisories are automatically created by Black Duck's Cyber Security Research Center using automated AI tools. These BDSAs have not been independently verified by the BDSA team but are created using automated processes and Generative AI assistance. These advisories are designed to supplement the BDSAs identified and verified by our Cyber Security Research Center.

You will find the AI Assisted tag in all areas where other vulnerability tags are found:

- As a filter on the Find page for vulnerabilities
- As a filter a project version's Security page
- As a Vulnerability condition for policies

New internal SSL certificate expiration alert

Black Duck 2024.7.0 introduces a new internal SSL certificate expiration alert. This alert notifies users 30 days in advance when their internal SSL certificates are approaching their expiration date, ensuring timely renewals and uninterrupted secure connections.

New SBOM retention configuration

When customers generate an SBOM that is meant to be distributed, it's important that an SBOM management solution retains the SBOM so it can be reproduced if needed. This is different than other type of Black Duck reports and while it typically happens as part of the release process at a point in time when no further changes are expected to the BOM, that’s not always the case.

Using this new feature, you can now configure the retention period for project version SBOM reports for both standard and LTS projects.

The SBOM retention settings can be configured in Admin → System Settings → Data Retention → SBOM Retention.

New option to filter indirect dependencies in SBOM templates

The SBOM Template now has an option to only include direct dependencies of components or components with no dependencies in the SBOM. This option can be found at the bottom of the Component Data section of the SBOM Templates page. The default state is unchecked and applies to both CycloneDX and SPDX report types. If unchecked, all components in the BOM are included.

Note: This information may only be available for certain components.

Improved copyright handling in reports

Black Duck 2024.7.0 brings significant improvements to the way copyrights are handled in SBOM and Notices File reports. Changes include:

- Enhancements to the algorithm used create lists of copyrights. The new algorithm will include previously missed copyrights, remove comment characters and make the entries more readable by replacing escaped character codes with real characters.
- Copyright lists which are now sorted alphabetically and removal of duplicate entries from the lists.
- More customizations for the Notices File report, including the ability to exclude license text and license data. The Notice File report now also includes a section displaying the selected options used when generating the content.
- A new Copyrights page in the Systems Settings which allows you to configure global copyright settings for SBOM and Notice File reports. Options include the ability to merge identical copyrights with different dates, remove copyright statements that do not include a date, or use a standard copyright tag.

Improved Notices File report

The Notice File report has been enhanced with the addition of home page URLs and clearer details when pertaining to components without a copyright. Starting in 2024.7.0, components without copyrights will display "No Copyrights found".

Binary matching for versionless components via fuzzy match

Binary Matching introduces new capabilities into Black Duck for identifying component versions from binary scans. This technique leverages a new SaaS matching service for binary scanning, identifying the closest component version match or matches when an exact match is not found through binary analysis. Match scores for component versions range from 4 (lowest score) to 100 (highest score).

This update also adds support for fuzzy match APIs. Binary matches that utilize fuzzy match component versions will show their respective match score and how many alternative matches were found. The scoring formula is sophisticated and further enhancements to this matching process will be implemented as part ongoing KnowledgeBase improvements along with ways to highlight the best possible match on the BOM.

Updated maximum binary scan size

We have increased the maximum size of binaries that can be scanned from 5GB to 20GB. This change addresses security restrictions in the Black Duck hosted environment, ensuring we maintain robust security while allowing the scanning of larger binaries.

Updated scan BOM Import Log

We have optimized the BOM Import Log for better performance and reduced storage costs:

- Records of missing, not found, or mapped licenses will no longer be recorded in the BOM import log.
- Only the most recent BOM import log will be retained.

These improvements streamline the logging process and focus on the most relevant data, ensuring a more efficient use of resources.

Updated project creation process

The project creation process has been updated as follows:

- If SCM Integration is not enabled on your server, clicking the Create Project button brings you directly to the create project form. There is no change in this circumstance.
- If SCM Integration is enabled, clicking the Create Project button now shows a dropdown with the options, Standard Project and SCM Project. Clicking Standard Project will bring the user to the create project form. While clicking SCM Project will bring the user to the SCM Server selection page.

Updated `component_vulnerability` table in the Reporting view

A new `remediation_updated_at` field has been added to the `component_vulnerability` table. This field records the date when the triage status of a vulnerability was last updated.

Binary scans migration to protobuf format

Traditional jsonid binary scans have been migrated to protobuf format introduced in 2023.10.0 for all scans with BDBA. No action is required to update your environment due to this migration, and scan results will remain unaffected.

Added SBOM fields to project settings and components

The following SBOM fields have been added:

- Originator: Projects, BOM Components
- Download Location: Component Version, Custom Component Version

Added macOS ARM64 support for Signature scanner

The Signature scanner now supports macOS ARM64. This update ensures compatibility across Black Duck products, providing improved performance and seamless operation for ARM64-based systems.

Removal of the "IN" operator for specified policy rule conditions

The following policy rule conditions no longer allow the “IN” operator. This change applies only on new and updated policy rules. Existing policies are not affected.

- New Versions Count
- Critical Severity Vulnerability Count
- High Severity Vulnerability Count
- Medium Severity Vulnerability Count
- Low Severity Vulnerability Count

Supported browser versions

- Safari Version 17.5
  - Safari versions 14 and below are no longer supported
- Chrome Version 126.0.6478.127 (Official Build) (x86_64)
  - Chrome versions 91 and below are no longer supported
- Firefox Version 128.0 (64-bit)
  - Firefox versions 89 and below are no longer supported
- Microsoft Edge Version 123.0.2420.97 (Official build) (64-bit)
  - Microsoft Edge versions 91 and below are no longer supported

Container versions

- 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
- blackducksoftware/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 enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Removal of deprecated matched components API request

The following deprecated API request has been removed in the 2024.7.0 release:

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

New vulnerable-bom-components version

A new version (V8) of the following API request has been added:

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

The latest version of this API request features improved performance and the following fix to enhance the quality of the output:

- The `vulnerabilityName` field has been removed from the `/api/projects/<project-id>/versions/<version-id>/vulnerable-bom-components` API request in the new lightweight version as `vulnerabilityName` and `vulnerabilityId` fields possessed same value and `vulnerabilityId` is more commonly used.

Binary scanner information

The binary scanner has been updated to version 2024.6.2.

Fixed issues

The following customer-reported issues have been fixed in this release:

- (HUB-34550). Fixed the way short numeric dates are display based on web browser locale. For example, European locales will now display day/month/year date format.
- (HUB-40168). Fixed copyright display issues. See Improved copyright handling in reports for more information.
- (HUB-40687). Fixed an issue where the last scanned time was not displayed correctly on the Find page.
- (HUB-40774). Fixed an issue where vulnerabilities with a CVSS 3 attack vector value of "adjacent network" were previously mapped in Black Duck with a null value. As of 2024.7.0 the value is properly mapped, and a one-time job will be triggered to fill in that data for any cached vulnerabilities with a null CVSS 3 attack vector field.
- (HUB-41220). Fixed an issue where the incorrect severity level could be displayed when searching for vulnerabilities on the Find page.
- (HUB-41264). Fixed an issue where the scan size displayed was inconsistent between the Scan page (with snippet matching) and the .CSV file generated when clicking 'Export Current View' button.
- (HUB-41348). Fixed an issue on the Scan page where the sorting of scans by size was incorrect when snippets are included.
- (HUB-41683). Removed the `vulnerabilityName` field from the `/api/projects/<project-id>/versions/<version-id>/vulnerable-bom-components` API request in the new lightweight version as `vulnerabilityName` and `vulnerabilityId` fields possessed same value and `vulnerabilityId` is more commonly used.
- (HUB-41851). Renamed a duplicate "Component Origin Id" column in the Version Details Report (Project Version Upgrade Guidance) to Component Origin External ID.
- (HUB-42041). Fixed an issue where once edits to a component details setting/license/custom field is made on the global level and you try to revert back to previous pages visited in Black Duck, it loses the navigation and never brings you back.
- (HUB-42054). Fixed an issue where the `/api/projects/{projectId}/versions/{projectVersionId}/risk-profile` API request was returning unknown security risk for ignored confirmed snippets match types on components tab.
- (HUB-42155). Fixed an issue where the Last Updated timestamp for project version auto-deletion was being erroneously modified by system computations and other project adjustments.
- (HUB-42225). Fixed an issue on the project version's Source tab where the Unmatched filter option displayed both unmatched files and unmatched components, which made it difficult to find unmatched components amongst the results. This filter has now been split into two separate values: Unmatched Files (displays only unmatched files) and Unmatched IDs (displays only unmatched component ids).
- (HUB-42260). Fixed an issue where the exploit available status of CVE vulnerabilities in the UI and in the vulnerability report may not match in certain circumstances.
- (HUB-42363). Fixed an issue where users with direct/indirect access to a project could not see layer information for container scans.
- (HUB-42402, HUB-42471). Fixed an issue where project versions without mapped scans were not being scheduled for project version auto-deletion.

- (HUB-42466). Fixed an issue where scanning a large project with a package manager scan could result in an output file containing over 10,000 graph nodes, potentially causing the scan container to eventually time out.
- (HUB-42478). Fixed an issue where the reporting database was not getting populated when using `hub_db_migrate.sh` due to `search_path` not being passed correctly in the definitions of the reporting database matviews.
- (HUB-42531). Fixed an issue where attempting to download system logs could generate a "Log files not found" error when deploying with read only YAML file.
- (HUB-42545). Fixed an issue where long term support (LTS) projects did not show up in the modal for adding projects to a project version, and when manually calling the API to do so, they did not appear in the list of components.
- (HUB-42753). Fixed an issue where binary matches incorrectly added an extra ID to the count set by the API for BOM matches. This discrepancy affected the match confidence, causing it to misalign with the number of alternatives in fuzzy matches.
- (HUB-42760). Fixed an issue where the Snippet Review Status column was missing when creating a Version Details report with the Components category added.
- (HUB-42811). Fixed a pagination issue where the `offset` value for the `vulnerable-bom-components` API endpoint was returning the same result regardless of what the value was set to.
- (HUB-42873). Fixed an issue where SBOM Copyright reports could fail due to not validating if the component exists in the BOM.
- (HUB-42953). Fixed an issue where the risk profile in the Version Details Report incorrectly used the operational risk medium count instead of license medium risk count.
- (HUB-43001). Fixed an issue regarding the documentation regarding the configuration of the automatic scan retry header.

Black Duck SCA 2024.4.x

Black Duck SCA 2024.4.1

Announcements

Upcoming OpenShift/Kubernetes documentation merger

With our 2024.7.0 release, we are transitioning our OpenShift support to utilize Kubernetes helm-based deployment. The current OpenShift standalone install guide will be discontinued and merged into the Kubernetes install guide, with sections tailored for OpenShift.

Black Duck will continue to be supported in OpenShift environments, but will need to use our Kubernetes helm chart configuration for installation and upgrades. Please refer to our installation documentation or contact Black Duck Support for any additional guidance.

New and changed features

Improved BOM import log

The BOM import log will now add any unmatched components without a PURL from an SBOM import to the BOM Import Log so it’s visible and actionable. The error messages now clearly indicate the reason why the particular component cannot be matched:

- If the PURL has no matches in the KnowledgeBase, the error message displayed is *Unable to map scanned component version to Black Duck project version because no mapping is present for the given external identifier*.
- If the PURL is invalid, the error message displayed is *Unable to map scanned component version to Black Duck project version because given external identifier is invalid*.
- If the PURL is missing, the error message displayed is *Unable to map scanned component version to Black Duck project version because no external identifier is provided*.

Improved ReversingLabs scan results

Black Duck 2024.4.1 includes an enhancement to our ReversingLabs malware scans. All malware scans will now include the specific malware threat name, providing you with more detailed and precise information about detected threats, and aims to enhance your ability to respond to security issues more effectively.

Please note, to take advantage of this new update, you must rerun the ReversingLabs scan to see the new threat name in the scan results.

Container versions

- 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:2024.4.1-RC
- blackducksoftware/blackduck-logstash:1.0.36
- blackducksoftware/bdba-worker:2024.3.0
- blackducksoftware/rabbitmq:1.2.37
- blackducksoftware/blackduck-authentication:2024.4.1
- blackducksoftware/blackduck-bomengine:2024.4.1
- blackducksoftware/blackduck-documentation:2024.4.1
- blackducksoftware/blackduck-integration:2024.4.1
- blackducksoftware/blackduck-jobrunner:2024.4.1
- blackducksoftware/blackduck-matchengine:2024.4.1
- blackducksoftware/blackduck-redis:2024.4.1
- blackducksoftware/blackduck-registration:2024.4.1
- blackducksoftware/blackduck-scan:2024.4.1
- blackducksoftware/blackduck-storage:2024.4.1
- blackducksoftware/blackduck-webapp:2024.4.1

API enhancements

There are no new or changed API requests in Black Duck 2024.4.1. For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Binary scanner information

There are no changes to the binary scanner in 2024.4.1.

Fixed issues

The following customer-reported issues were fixed in this release:

- (HUB-39354). Fixed an issue where the Project Alias field in the Software Bill of Materials (SBOM) only overrode the Main Project name and Version at the Project level and did not extend to subprojects included in an SBOM report.
- (HUB-39807). Fixed an issue where the vulnerable-bom-components API endpoint in the UI could hang indefinitely.
- (HUB-41575). Fixed an issue where archive files being downloaded from the Scan list were downloaded with the wrong file type, resulting in an error when uploading as a BDIO file.
- (HUB-41670). Fixed an issue where the scan pod was having difficulties accessing the rabbitmq admin plugin to allow for the retry attempts to occur on hosted environments with rate limiting enabled.
- (HUB-41753). Fixed an issue where the `DESCRIBES` relationship was missing from the SPDX SBOM report exports.
- (HUB-41992). Fixed an issue where custom fields containing the "/" character could cause a blank list of conditions when creating policies for those custom fields.
- (HUB-42086). Fixed an issue where the `api/versions/<versionID>/reports` endpoint was displaying unclear information in the `riskProfile` section of the API output.
- (HUB-42101). Fixed an issue where the VULNERABILITY_REPRIORITIZATION job could get stuck when processing entries without a cvss3 score.
- (HUB-42158). Fixed an issue where the SBOM SPDX report was not displaying the correct license name for "SSLeay License - standalone".
- (HUB-42208). Fixed an issue where the Error Status filter was missing on Jobs page on some instances.
- (HUB-42304). Added an index for the `st.version_bom_entry(code_location_id)` table to help alleviate the pressure against the specific table in question.
- (HUB-42334). Fixed a sorting order issue on the Malware tab of the project version page which could result in duplicate rule ID entries.
- (HUB-42382). Fixed an issue where the Source tab did not redisplay matches after deselecting matched item in File Tree.
- (HUB-42585). Fixed an issue where new SAML and LDAP user accounts could not authenticate properly when added to the designated default user group.

Black Duck SCA 2024.4.0

Announcements

Updated operating system support

The preferred operating systems for installing Black Duck 2024.4.0 have been updated as follows:

- End of support for CentOS 7.
- End of support for Red Hat Enterprise Linux server 7.9 and 8.6.

- Added support for Red Hat Enterprise Linux server 8.9 and 9.x.

Deprecation and upcoming removal of the allow/deny nginx configuration

Black Duck 2024.4.0 has deprecated the following features built in to blackduck-nginx:

- DENY_ACCESS_DIRECTIVES
- ALLOW_ACCESS_DIRECTIVES

These features will be fully removed in Black Duck 2024.7.0.

Documentation localization

The 2024.1.0 version of the UI, online help, and release notes have been localized to Japanese and Simplified Chinese.

New and changed features

Preliminary support for PostgreSQL 16

Black Duck 2024.4.0 adds preliminary support for using PostgreSQL 16 as an external database. This support is for *testing only*; production use IS NOT SUPPORTED.

New malware scans

scans allow you to get access to enhanced malware and threat intel data via our partnership. Using complex binary analysis powered by , developers and DevOps teams can analyze first party, open source, and commercial software to identify the presence of threats such as malware, maldocs, suspicious files, potentially unwanted applications (PUAs), protestware, and suspicious file structure malformations to help avoid dangerous software supply chain attacks.

New Unmatched component auto-creation

In an SBOM management workflow, the SBOM is the input and all of the components included in the SBOM need to be persisted in the SBOM management solution so that visibility isn't lost, regardless if there is a match to the KnowledgeBase. This feature provides the option to automatically create unmatched components in the BOM with custom components of the same name in an SBOM import as long as the component has an associated PURL in the SBOM.

In addition, you also have the ability to configure the default license applied to auto-created components where the SBOM license tag value is NOASSERTION.

New SBOM templates

SBOM Templates is a new feature that effectively replaces and enhances the ability to determine what is included in an SBOM report. The SBOM Template allows users to select which of those fields they want to include in the generated SBOM as well as some other configuration items like whether to include vulnerability info (for CycloneDX) or Dev/Build tools. SBOM templates can then be selected when creating SBOM reports to generate desired outputs.

Please note, some SBOM field configurations were moved from project group settings to the SBOM template configuration. Customers are encouraged to review and configure SBOM templates after upgrading to Black Duck 2024.4.0 before generating new SBOM reports.

Added new CLI command line option for project groups

You can now add the `--project-group` option to the Signature Scan command line which sets the 'Project Group' to assign the project to. If the project doesn't already exist, a new project will be created in the corresponding project group.

This parameter has no effect if the project already exists or if the specified project group does not exist.

Added support for CycloneDX 1.5

You can now export the Software Bill of Materials report for your projects in CycloneDX v1.5 format. This can be done by viewing a project version, clicking the Reports tab, clicking the Create Report button, and then selecting CycloneDX v1.5 - JSON. For more information on CycloneDX v1.5, please visit the CycloneDX v1.5 reference page.

Enhanced missing container scan registration error handling

Container scans will now fail with an appropriate message if your Black Duck registration key does not have Container Scanning enabled.

Enhanced SBOM import error handling

SBOM import error handling has been improved to provide better visibility as to why an SBOM import may have failed, including specific lines/fields that failed the validation. In addition, you can export the failure to a log file so that it can be researched outside of the Black Duck UI and re-import attempted after the necessary updates have been made to the SBOM.

Updated method of setting HUB_MAX_MEMORY

Starting with Black Duck 2024.4.0, the configuration parameter `HUB_MAX_MEMORY` is automatically set for relevant containers in Kubernetes-based deployments. The value is computed as a percentage of the memory limit, with 90% being the default. In the gen04 deployment sizings, the `hubMaxMemory` setting has been replaced with `maxRamPercentage` to control the percentage used; the values for this setting were chosen so that `HUB_MAX_MEMORY` has the same values as before.

This change does not apply to Swarm-based deployments.

Updated match score confidence for components imported via SBOM

When viewing a project version's BOM where components were imported from a SBOM file, the match score displayed will always be 100% and the match type will indicate SBOM as the origin.

Updated binary match type results with BDBA package manager support

Previously, all container and binary scans produced a single binary match type. With the expanded package manager support from BDBA, we can now identify additional match types based on the BDBA matching method. As a result, you will see changes in your BOM, with components identified through binary and container scanning gaining or changing their match types.

Removal of the blackduck-webui container

The blackduck-webui container has been removed and its builds are now included in the blackduck-nginx container. The blackduck-nginx container will now follow the same release cadence as the rest of the blackduck stack.

Supported browser versions

- Safari Version 17.4.1
  - Safari versions 14 and below are no longer supported
- Chrome Version 123.0.6312.124 (Official Build) (x86_64)
  - Chrome versions 91 and below are no longer supported
- Firefox Version 124.0.2 (64-bit)
  - Firefox versions 89 and below are no longer supported
- Microsoft Edge Version 123.0.2420.97 (Official build) (64-bit)
  - Microsoft Edge versions 91 and below are no longer supported

Container versions

- 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
- blackducksoftware/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 enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

New component filter keys for SBOM creator and SBOM name fields

New filter keys have been added to the following API request which return the possible values for BOM components' SBOM names and creators.:

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

Filter keys:

- `sbomName`
- `sbomCreator`

New component filtering support for SBOM creator and SBOM name fields

New filters have been added for the following API request:

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

Filters:

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

New snippet matching REST API request (Generative AI Compliance)

The following API request has been added which allows you to find snippet matches for a given code snippet:

- `POST /api/snippet-matching`

These matches are sorted by license family to better display the risk a particular match represents (`PERMISSIVE`, `WEAK_RECIPROCAL`, `RECIPROCAL`, `RECIPROCAL_AGPL`, `RECIPROCAL_NETWORK`, `UNKNOWN`).

Deprecation of matched component API request

The following matched component API request has been deprecated and will be removed in Black Duck 2024.7.0:

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

Binary scanner information

The binary scanner has been updated to version 2024.3.0.

Fixed issues

The following customer-reported issues were fixed in this release:

- (HUB-39206). Fixed an issue where the binary scanner was not detecting .DEB file components causing them to not appear in the resulting report.
- (HUB-39395). Fixed an issue where KnowledgeBase updates was showing the Last Updated user as the user who added the component in Component Management. Custom components updated by KnowledgeBase update jobs will now display as System User.
- (HUB-39635). Fixed an issue when a Detect CONTAINER_SCAN was run in conjuction with other scan types (e.g. DETECTOR or BINARY_SCAN), Detect was not returning the expected `412 Precondition Failed` error message.
- (HUB-40531). Fixed an issue where component reports could produce duplicate entries for some components.
- (HUB-40745). Fixed aSPDX SBOM report issue where the PackageSupplier field may be different from the origin name in the Purl field when there are multiple origins for a same component version in the BOM.

- (HUB-40769). Deprecated the API request GET /api/projects/{projectId}/versions/{projectVersionId}/matched-components as it was returning a 404 error when used.
- (HUB-40870). Fixed an issue when constructing the URL encoding the search parameters of the ‘origins-with-filters' link leading to the component's Copyright page.
- (HUB-40930). Fixed an issue in localized CSV files where garbled characters were displayed when opening search results in Excel.
- (HUB-40998). Fixed an issue where thePackage Valid Until Date field in SBOM report was not being cleared when removed by the user.
- (HUB-41041). Fixed a broken link in the SCAaaS helm chart readme file.
- (HUB-41063). Fixed an issue where only "Direct Dependency" would show if both "Transitive" and "Direct" matches existed within the same component version.
- (HUB-41132). Fixed an issue where searching for components containing the + special character could not return the expected results.
- (HUB-41167). Fixed the REST API documentation concerning the supported filters of the Listing Project Versions API. The only supported filters are phase, license, and distribution.
- (HUB-41276). Fixed an issue where components with Unknown Licenses would not be included into the Notices File report.
- (HUB-41299). Fixed an issue where custom components that were previously mapped and then deleted were being remapped erroneously, affecting unmatched components totals in subsequent scans.
- (HUB-41316). Fixed an issue where upgrading SaaS to 2023.7.3 could cause SSO to fail.
- (HUB-41318). Fixed an issue with inconsistent behavior when searching component versions.
- (HUB-41321). Fixed an issue where comments for snippet results in .ZIP files were not exported to the source report.
- (HUB-41362). Fixed an issue where the Discovery filter was displaying all discoveries instead of the search results based on the text typed into the search field.
- (HUB-41365). Fixed an issue when the `/api/projects` limit is set to 0 (`/api/projects?limit=0`) could cause the resulting page to never load.
- (HUB-41369). Fixed an issue where uploaded branding logos were not automatically scaled down to fit the size requirements as intended.
- (HUB-41391). Fixed an issue where incorrectly formed PURL fields in a SBOM could cause CycloneDX to fail importing the SBOM file.
- (HUB-41431). Fixed a documentation issue related to the Project Manager role and project deletion permissions.
- (HUB-41450). Updated the readme file to correctly the ordering of values.yaml file before the sizing.yaml in the deployment command.
- (HUB-41461). Fixed an issue where the Total Count displayed when using the Listing Affected Project Versions API was the number of projects, not project versions.
- (HUB-41502). Resolved security issues found in the SCAaaS deployment.
- (HUB-41542). Fixed an issue where the BOM Last Updated date was being reset by kbupdatejob component update on fuzzy BDBA scans.
- (HUB-41549). Fixed a localization issue when exporting the users list in CSV format.

- (HUB-41552). Fixed an issue with the Project Version Auto-Deletion function interaction with the Retain Project Version regardless of data retention policies when it is disabled and the system is restarted.
- (HUB-41570). Fixed an issue where the `scan_stats_view` materialised view taking excessive amount of time to execute.
- (HUB-41591). Fixed a deadlock issues in the HUB CloudSQL database caused by delete queries.
- (HUB-41773). Fixed an issue when attempting to upload multiple files in a folder and dragged them on the Upload SBOM-SPDX File or Upload SBOM-CycloneDX File.
- (HUB-41867). Fixed an issue where any vulnerability notification generated by KB Update job and BOM Package Adjustment (User manually mapped an unmatched external ID in a BOM to a KB component) had the incorrect "Unknown" event source.
- (HUB-41930). Fixed an issue where the nginx webserver would not start unless the user running the pod is either root (0) or nginx (101).
- (HUB-41974). Fixed an issue with the Unmatched Filter on the Project Version -> Source Tab displaying incorrect counts.
- (HUB-42004). Fixed an issue where access a page in Black Duck immediately after SSO login would not take the user to the intended page.
- (HUB-42051). Fixed an issue where the value of `download_location` in `version_bom_component` was not removed when the component download location in the UI was cleared.

Black Duck SCA 2024.1.x

Black Duck 2024.1.1

Announcements

Black Duck 2024.1.0 Job runner issue (HUB-41654)

A high impact bug (HUB-41654) was identified in 2024.1.0 which affects the Black Duck Job runner and KnowledgeBase Update Check job. This bug causes the Update KnowledgeBase Data job to fail to apply updates to BOMs with new or modified vulnerabilities. This issue will only occur when specific vulnerability conditions apply and is likely to only impact a small number of customer BOMs. We recommend customers running 2024.1.0 upgrade to 2024.1.1 as soon as possible to resolve this issue.

This issue only impacts customers running 2024.1.0. For further details, please see the Community announcement regarding this issue.

New and changed features

New Project Version SBOM field configuration

You can now configure project version SBOM fields to define the BOM component SBOM fields when a component is used as a sub-project for a project version so that the appropriate level of detail is provided in the SBOM without having to define it for every project the sub-project is used in.

Updated search functionality

The algorithm used for searching in Black Duck has been enhanced and will broaden the scope of the search to make it easier for you to find the information you need by enabling the retrieval of all records

containing strings or partial matches. It will provide results similar to those obtained using a Solr search, allowing you to find relevant records even if you do not know the complete string.

Container versions

- 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
- blackducksoftware/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 enhancements

Updated project version policy rule summary API

A new version of the project version policy rule summary API has been added which offers a paginated list of policy rule violations and their associated BOM component count:

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

The previous version has been deprecated, and will be removed in an upcoming Black Duck release.

Updated BOM vulnerability endpoint

A new version (V8) of the vulnerable BOM components endpoint has been added which contains performance improvements:

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

Version 8 of the endpoint only contains the minimum amount of data to serve current UI/UX views or custom integration utility in order to produce faster results and prevent timeout failures. Note that V7 of this API endpoint also exists and mapped to the existing V6.

Binary scanner information

There are no changes to the binary scanner in Black Duck 2024.1.1.

Fixed issues

The following customer-reported issues were fixed in this release:

- (HUB-38966). Fixed an issue where policy evaluation could fail due to missing risk data involving the policy expression is Newer Versions Count.
- (HUB-40443). Fixed an aggregator function issue with policy violations discrepancies between UI and reports.
- (HUB-40666). Fixed an issue where license assignment might not update when the KbUpdate License Job finishes.
- (HUB-40690). Fixed issues arising with rabbitmq update which could cause false failure errors on Kubernetes.
- (HUB-40861). Fixed an issue where searching for components within Black Duck with a "dash" symbol and spaces were not returning results unless double spaced.
- (HUB-40975). Fixed an issue where attempting to bulk edit unmatched components could generate an error message (The application has encountered an unknown error).
- (HUB-41054). Fixed an issue where a project versions's source report could output duplicated entries.
- (HUB-41069). Fixed an issue where the Supplier field was not present on CycloneDX SBOM reports.
- (HUB-41281). Fixed an issue where components were being truncated when clicking the 'Print' button in BOM reports.
- (HUB-41295). Fixed an issue where the Create button was missing on the Create Custom Fields page when logged in as a non-System Administrator user.
- (HUB-41347). Fixed an issue where version-specific scan retention setting was available when the global setting was disabled.
- (HUB-41390). Fixed an issue where an error could occur when an excessive number of parameters is used with the /api/internal/dashboard-facts API request.
- (HUB-41396). Fixed an issue causing the Update KnowledgeBase Data job to fail to apply updates to BOMs with new or modified vulnerabilities. See the related announcement for more information.
- (HUB-41463). Fixed an issue where the BDBA worker log was not being captured from system logs.
- (HUB-41502). Updated the following SCAaaS component versions to resolve security vulnerabilities:

Component Name	Previous Version	New Version
com.fasterxml.jackson.core:jackson-core	2.13.3	2.14.1
com.fasterxml.jackson.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

Component Name	Previous Version	New Version
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 SCA 2024.1.0

Announcements

Removal of upload-cache service

Encryption is now handled by the Black Duck secrets encryption libraries and key rotation mechanisms. As a result, the `recover_master_key.sh` and `bd_get_source_upload_master_key.sh` scripts for handling SEAL_KEY changes have been removed.

Also, uploaded source files used by the Source tab in Black Duck are not migrated. If needed, you can rescan the source in an existing or new, temporary project. Note that source uploads must still be explicitly enabled with `ENABLE_SOURCE_UPLOADS` (default false) and are still deleted automatically to meet the `MAX_TOTAL_SOURCE_SIZE_MB` (default 4G) and `DATA_RETENTION_IN_DAYS` (default 180 days) configuration settings.

NOTE: Uploaded source code will not be migrated by default and migration scripts are not included as part of the Black Duck 2024.1.0 release. Please contact Black Duck Support if you require your uploaded source code migrated as part of your upgrade.

Scanning hardware requirements changes

Black Duck 2024.1.0 will see a number of changes in scanning hardware requirements therefore Black Duck customers will need to update their environments and allocate additional hardware resources where necessary per the guidance below.

Please see Black Duck Hardware Scaling Guidelines for more information.

Table 1: Hardware Scaling Guidelines

Name	Details	
120sph	**Scans/Hour**: 120 **SPH % Increase**: 0% **APIs/Hour**: 3,000 **Project Versions**: 13,000	**IOPS**: Read: 15,000 / Write: 15,000 **Black Duck Services**: CPU: 11 core / Memory: 56 GB **PostgreSQL**: CPU: 4 core / Memory: 16 GB **Total**: CPU: 15 core / Memory: 72 GB
250sph	**Scans/Hour**: 300 **SPH % Increase**: 20% **APIs/Hour**: 7,500 **Project Versions**: 15,000	**IOPS**: Read: 15,000 / Write: 15,000 **Black Duck Services**: CPU: 16 core / Memory: 86 GB **PostgreSQL**: CPU: 6 core / Memory: 24 GB **Total**: CPU: 22 core / Memory: 110 GB
500sph	**Scans/Hour**: 650 **SPH % Increase**: 30%	**IOPS**: Read: 25,000 / Write: 25,000 **Black Duck Services**: CPU: 23 core / Memory: 133 GB

Name	Details	
	APIs/Hour: 18,000 **Project Versions**: 18,000	**PostgreSQL**: CPU: 16 core / Memory: 64 GB **Total**: CPU: 39 core / Memory: 197 GB
1000sph	**Scans/Hour**: 1400 **SPH % Increase**: 40% **APIs/Hour**: 26,000 **Project Versions**: 25,000	**IOPS**: Read: 25,000 / Write: 25,000 **Black Duck Services**: CPU: 46 core / Memory: 367 GB **PostgreSQL**: CPU: 22 core / Memory: 88 GB **Total**: CPU: 68 core / Memory: 455 GB
1500sph	**Scans/Hour**: 1600 **SPH % Increase**: 6% **APIs/Hour**: 41,000 **Project Versions**: 28,000	**IOPS**: Read: 25,000 / Write: 25,000 **Black Duck Services**: CPU: 57 core / Memory: 459 GB **PostgreSQL**: CPU: 26 core / Memory: 104 GB **Total**: CPU: 80 core / Memory: 563 GB
2000sph	**Scans/Hour**: 2300 **SPH % Increase**: 15% **APIs/Hour**: 50,000 **Project Versions**: 35,000	**IOPS**: Read: 30,000 / Write: 30,000 **Black Duck Services**: CPU: 64 core / Memory: 565 GB **PostgreSQL**: CPU: 32 core / Memory: 128 GB **Total**: CPU: 96 core / Memory: 693 GB

Documentation localization

The 2023.10.0 version of the UI, online help, and release notes have been localized to Japanese and Simplified Chinese.

New and changed features

New Black Duck Automated Security Advisories (ASA)

Automated Security Advisories (ASA) are automatically created by Black Duck's Cyber Security Research Center using automated AI tools. ASAs are created from various trusted security feeds such as the GitHub Security Advisories (GHSA) feeds along with automated vetting using AI tooling. These advisories are designed to supplement the BDSAs identified and verified by our Cyber Security Research Center.

You will find ASA-tagged BDSAs in all areas where other vulnerability tags are found.

New Download Location value for a BOM Component

A new Download Location SBOM field has been added to the list of Additional Fields. The Download Location is found under the BOM Component section and is configurable, allowing you to add the URL or other specific location within a version control system (VCS) where the component was downloaded. This new information is displayed in the SBOM report as:

- SPDX: Under the `packages` > *`package ID`* section as `downloadLocation`.
- CycloneDX: Under the `components` > `externalReferences` section as `url`.

New copyright text, license comment, and homepage data for SBOM reports

The available SBOM report options under project group settings were updated to support inclusion of copyright data, license comments, and homepage URL to the SBOM reports. Copyright text, license comments, and homepage URLs are included in both CycloneDX and SPDX reports if the group setting is enabled.

New SCM repository auto-scanning

SCM repository auto-scanning allows Black Duck to check daily for any changes such as commits, pushes, or merges in the repository branch mapped to your SCM projects and perform scans if changes were made. To take advantage of this feature, you must enable it through to Admin → Jobs → Scheduled.

In addition, two new SCM repository auto-scanning jobs have been added to Black Duck to support this feature:

- SCM Onboarding daily auto scanning: Schedules nightly job that performs auto scanning of previously onboarded SCM repositories.
- SCM Onboarding daily cleanup: Schedules nightly job that cleans up from SCM Onboarding.

Added CISA Known Exploited Vulnerability tag

Vulnerabilities listed in the CISA Known Exploited Vulnerability Catalog are now tagged as such in Black Duck. This allows you to add CISA Known Exploited Vulnerabilities as a Vulnerability Conditions policy filter. Please visit CISA's Known Exploited Vulnerability Catalog page for more information.

Updated SCM integration

Black Duck 2024.1.0 has added two new SCM providers to the list of SCM integrations:

- GitLab SaaS
- Bitbucket

You can now add these authorized SCM providers which can then be selected when creating a new project. Doing so will automatically pre-populate the repository URL and branch version in the Project Settings page for your new project.

This feature is compatible with Detect 8.x and above, and will take effect with new package manager scans.

Please note that SCM integration is not enabled by default in Black Duck and must be activated by adding the following in your environment:

For Swarm users, add the following to your `blackduck-config.env` file:

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

For Kubernetes users, add the following to your `values.yaml` file under the environs section:

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

Updated SBOM report relationship information

SBOM reports were updated to add dependency information. SPDX reports the dependencies now include the dependency type in the `relationships` section. Note that this applies only to SPDX 2.3 reports. CycloneDX reports do not include dependency types.

Updated deep license data management for snippet component matches

Customers leveraging Deep License Data (DLD) and snippet matching together can now configure their projects to see deep license risk appearing for files present in the components found in their code.

The feature has been broken up into two separate functions:

- **Apply Deep License Data to Bill of Materials**: Enabling this checkbox will apply deep license data to your non-snippet components and allow visibility to embedded licenses which may exist in your components beyond declared licenses.
- **Apply Deep License Data to Snippet Component Matches**: If enabled, component snippet matches are included in the deep license data calculation.

Enhanced license conflict management for project hierarchies

Previously, license conflicts were calculated only from a single project license and did not factor in project hierarchies. With Black Duck 2024.1.0, subprojects within the parent project will now also factor in the calculation.

Hierarchical licence conflicts are enabled by default with Black Duck 2024.1.0 but can be configured in your environment. However, license conflict information is not automatically enabled. System Administrators must enable the Legal and License Conflicts tab to view license conflicts. Use the project's Settings tabs to enable the feature for current projects.

Enhanced component vulnerability history graph

The Vulnerability History graph displayed on a component's page now includes data for vulnerabilities of unknown origin.

Enhanced Kubernetes probes for SCA

Improvements have been made to the readiness probes used in Kubernetes environments:

- A new startupProbe has been added to verify whether the application within a container is started. The startupProbe runs before any other probe, and, unless it finishes successfully, disables other probes.
- The readinessProbe now starts checking after a 30 second initial delay (from 240 seconds) and checks every 10 seconds (from 30 seconds). It also allows for 15 failures before a restart is issued.
- The livenessProbes now checks every 10 seconds (from 30 seconds).
- New toggles for startupProbe and readinessProbes have been added. A unique flag has been added to control each probe.

Enhanced on-demand job retries

On-demand jobs previously attempted to retry three times before finally failing which, in some cases, could lead to situations where a job that is known to fail would continue to re-run and consume system resources. We have refined this approach by disabling retries by default so that jobs kicked off by the periodic scheduler retry when the corresponding check job runs again.

Please note that this change does not affect report jobs. Report jobs will retry as normal.

Change to the upload cache for source code upload

NOTE: This change was part of Black Duck 2023.10.0 and was not clearly communicated at the time.

In Black Duck 2023.4.2, a workaround was added for users running on AWS to deal with an issue where uploading source files and using the license search feature was not working due to file system latency and spawning of multiple du processes.

This issue was resolved in Black Duck 2023.10.0 with an architectural change to how Black Duck uses the upload cache and storage service. The upload cache is no longer used for the source code upload functionality in Black Duck therefore the root cause problem was eliminated with the new architectural model of the source code upload via the storage service.

New Detect GUI release

Detect GUI has been updated to version 2024.1.0 which includes Black Duck Detect (CLI) 9.1.0.

Supported browser versions

- Safari Version 17.1.2
  - Safari versions 14 and below are no longer supported
- Chrome Version 120.0.6099.216 (Official Build) (x86_64)
  - Chrome versions 91 and below are no longer supported
- Firefox Version 121.0.1 (64-bit)
  - Firefox versions 89 and below are no longer supported
- Microsoft Edge Version 120.0.2210.121 (Official build) (64-bit)
  - Microsoft Edge versions 91 and below are no longer supported

Container versions

- 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
- blackducksoftware/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 enhancements

There are no new or changed API requests in Black Duck 2024.1.0. For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Binary scanner information

The binary scanner has been updated to version 2023.12.1.

Fixed issues

The following customer-reported issues were fixed in this release:

- (HUB-37413). Resolved an issue with using upload source code in AzureFile as SC. The upload-cache service has been removed entirely, replaced by the storage service.
- (HUB-38991). Fixed an inconsistent display issue on the Scans page when counting the size of code location.
- (HUB-39012). Fixed a REST API issue when updating the component version approval status with an invalid value, the Approval Status would be set to "UNREVIEWED".
- (HUB-39160). Fixed an issue where Black Duck did not verify that a project version is part of a project if the URL is manipulated. Doing so will now return a HTTP 404 error page.
- (HUB-39361). Fixed an issue where timestamps only appeared as a tooltip in the Scans table.
- (HUB-39378). Fixed an issue where edits of BOM component usage were sometimes ignored if the component had multiple matches with different usages.
- (HUB-39736). Fixed a performance issue with the KB API `/component/<uuid>/versions` endpoint.
- (HUB-39864). Fixed an issue where BOM component edit could delete multiple origins if the component had multiple origins per match,
- (HUB-39948). Fixed a bomengine deadlocking issue caused by concurrently deleting a project and a corresponding code location.
- (HUB-39959). Fixed a validation issue with the IDP URL or XML. The UI will now display a proper error message and will not change the system if the IDP validation fails.
- (HUB-39983). Fixed an issue where rescan a repository where a failed scan could cause a 412 error in the Black Duck UI. The scanning workflow has been improved to better handle errors occurring during the scanning process.
- (HUB-39987). Fixed an issue where the Last Scanned Date and Updated Date was empty on SCM Project Versions.
- (HUB-40104). Fixed an issue where the Cryptography tab of a component could display a blank page if Cryptography was registered and then unregistered on a user's product registration key.
- (HUB-40667). Fixed an issue where project policy violations by tier on the Summary dashboard view could not populate any information.
- (HUB-40685). Fixed an issue where the Detect rate limiting parameters missing from the Black Duck documentation.
- (HUB-40898). Fixed a localization issue where the Maximum Snippet File Size was displaying an incorrect value.

Black Duck SCA 2023.10.x

Black Duck version 2023.10.2

- Announcements
- New and changed features

- API enhancements
- Binary scanner information
- Fixed issues

Announcements

There are no new announcements for Black Duck 2023.10.2.

New and changed features

There are no new or changed features in Black Duck 2023.10.2.

Container versions

- 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
- blackducksoftware/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 enhancements

There are no new or changed API requests in Black Duck 2023.10.2. For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Binary scanner information

There are no changes to the binary scanner in 2023.10.2.

Fixed issues

The following issues were fixed in this release:

- (HUB-40763). Fixed an intermittent issue where logging into Black Duck via SSO page could cause an authenticaton error after some time if the user did not log in immediately.
- (HUB-40944). Readded missing `created_at` and `updated_at` columns in the component table of the Reporting database.
- (HUB-40960). Fixed an issue where build packages in the manifest file were being captured by the Binary Scanner.

Black Duck version 2023.10.1

- Announcements
- New and changed features
  - API enhancements
  - Binary scanner information
  - Fixed issues

Announcements

Documentation localization

The 2023.7.0 version of the online help and release notes have been localized to Japanese and Simplified Chinese.

New and changed features

Updated Sigma version 2023.9.0

Sigma 2023.9.0 contains a fix for scanning Dockerfile extensions.

Container versions

- 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
- blackducksoftware/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 enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Updated response for matched-file API requests

The following API requests now have a `uri` field include in their responses:

- `/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`

Binary scanner information

There are no changes to the binary scanner in 2023.10.1.

Fixed issues

The following customer-reported issues were fixed in this release:

- (HUB-37681). Added the missing public API: `api/projects/{projectId}/versions/{versionId}/bom-status/{scanId}`to the REST API Developers Guide.
- (HUB-39616). Updated the API response for `matched-files` queries to include a `uri` field. See the API enhancements section for more information.
- (HUB-39693). Moved log messages related to symlink to the Trace level when using scan cli.
- (HUB-40316). Fixed an issue where the scan client could fail to write data to the BDIO file when the file name was blank. Validation has been added to verify that the file name is present and not a null string.
- (HUB-40354). Clarified the Notices File report documentation regarding sub-project name and license handling.
- (HUB-40524). Clarified the documentation regarding Detect Hosting Location for Internally Hosted options.
- (HUB-40631). Fixed an issue where a null pointer exception could occur when generating a Version Details report if a project version is added to another project as a subproject and the subproject doesn't have a nickname.

Black Duck version 2023.10.0

- Announcements
- New and changed features
  - API enhancements
  - Binary scanner information
  - Fixed issues

Announcements

Security Advisory for curl and libcurl (CVE-2023-38545, CVE-2023-38546)

Black Duck is aware of the security issue relating to curl and libcurl which was disclosed by the maintainer and original creator of the project on October 3, 2023.

CVE-2023-38545 impacts curl versions 7.69.0 through and including 8.3.0 and addresses a buffer overflow flaw that impacts both libcurl and the curl command line tool. The overflow can occur during a SOCKS5 handshake. If the handshake is slow, a user-supplied, unusually long hostname may not be resolved, and instead be copied into a target buffer for which it may exceed the allocated size. Heap-based buffer overflows such as these are known to lead to crashes, data corruption, and even arbitrary code execution.

CVE-2023-38546 is associated with a cookie injection flaw, but curl maintainers suggest that the series of conditions that must be met makes the likelihood of exploitation low. The versions impacted by this vulnerability are 7.9.1 through and including 8.3.0. Upgrading to curl 8.4.0 resolves the issue. Users are also advised to call curl_easy_setopt(cloned_curl, CURLOPT_COOKIELIST, "ALL"); after every call to curl_easy_duphandle();.

We believe that there is limited exposure to Black Duck' products, services and systems. To the extent we have had exposure, we have upgraded to the latest version of curl to remediate the situation.

For more information, please visit:

- Preparing for critical libcurl and curl vulnerabilities (CVE-2023-38545)
- How to respond to the curl and libcurl vulnerabilities

PostgreSQL 14 container migration

Black Duck 2023.10.0 supports upgrading from versions using either the PostgreSQL 11 container (versions 2022.2.0 through and including 2022.7.x) or the PostgreSQL 13 container (versions 2022.10.0 through and including 2023.7.x). During installation, the `blackduck-postgres-upgrader` container will migrate the existing database to PostgreSQL 14 and then exit upon completion.

Customers with non-core PG extensions are STRONGLY encouraged to uninstall them before migrating and reinstall them after the migration completes successfully; otherwise, the migration is likely to fail.

Customers with replication set up will need to follow the instructions in the pg_upgrade documentation BEFORE they migrate. If the preparations described there are not made, the migration will likely succeed, but the replication setup will break.

Customers not using the Black Duck-supplied PostgreSQL image will not be affected.

NOTE: Starting with 2023.10.0, Black Duck will only support direct upgrades from Black Duck versions that use the PostgreSQL 11 or PostgreSQL 13 containers (i.e., all Black Duck versions between 2022.2.0 and 2023.7.x inclusive). Users of the Black Duck-provided PG container upgrading from older Black Duck versions (i.e., all Black Duck versions prior to 2022.2.0) will require a 2-step upgrade: upgrade to 2023.7.x and then upgrade to 2023.10.x.

IMPORTANT: Before starting the migration:

- Ensure that you have an extra 10% disk space to avoid unexpected issues arising from disk usage due to the data copying of system catalogs.
- Review root directory space and volume mounts to avoid running out of disk space as this can cause Linux system disruptions.

For Kubernetes and OpenShift users:

- On plain Kubernetes, the postgres-upgrader init container within the PostgreSQL pod will run as root. However, the only requirement is that the container runs as the same UID as the owner of the PostgreSQL data volume.
- On OpenShift, the postgres-upgrader init container assumes that it will run with the same UID as the owner of the PostgreSQL data volume.

For Swarm users:

- The migration is completely automatic; no extra actions are needed beyond those for a standard Black Duck upgrade.
- The `blackduck-postgres-upgrader` container MUST run as root.
- On subsequent Black Duck restarts, `blackduck-postgres-upgrader` will determine that no migration is needed and immediately exit.

End of support for PostgreSQL 13

Support for PostgreSQL 13 has ended with Black Duck 2023.10.0. Please refer to the PostgreSQL Upgrade Schedule page for more information.

End of life for Black Duckctl

As of the 2023.7.0 release, Black Duckctl will no longer be supported and there will be no more updates. Documentation for Black Duckctl can be found at https://github.com/blackducksoftware/hub/tree/master/kubernetes/blackduck.

Please note that this announcement was accidentally left out of the Black Duck 2023.7.0 release notes.

Upgrade restrictions for PostgreSQL container users

Black Duck 2023.10.0 now only support direct upgrades from Black Duck versions that use the PostgreSQL 11 or PostgreSQL 13 containers (i.e., all Black Duck versions between 2022.2.0 and 2023.7.x inclusive). Users of the Black Duck-provided PG container upgrading from older Black Duck versions (i.e., all Black Duck versions prior to 2022.2.0) will require a 2-step upgrade: upgrade to 2023.7.x and then upgrade to 2023.10.x.

Documentation localization

The 2023.7.0 version of the UI have been localized to Japanese and Simplified Chinese. The localized formats for the online help and release notes will be available in an upcoming release.

New and changed features

New GitHub SCM repository scanning and read-only BOM

You can now integrate Black Duck with your GitHub repository, to quickly and easily gain visibility across all the repositories in GitHub, as well as the ability to add as a project version BOM in Black Duck.

You can now do the following:

- **Add selected main repositories as a new project in Black Duck**: This allows users to quickly view the security and policy violation of the GitHub repository.
- **Run scans at will:** You can trigger a scan from the Black Duck version page that is mapped to the repository, to find any new problems in your current libraries, for example to find critical zero-day vulnerabilities quickly. The result of this scan creates a lighter, read-only BOM which provides a quick overview of your repository detailing the components and licenses found, and any vulnerabilities associated to those components.

Please note that this feature is currently only supported for Hosted Black Duck customers. SCM integration utilizes a service that runs strictly within a Kubernetes environment, either native or Kubernetes in Docker (KinD). The helm charts will need to be used to install Black Duck to use this feature.

New scan auto-unmapping management page

You can now manage when scans are scheduled to be unmapped from inactive project versions. They need to meet the project version phase and inactivity time conditions, and will only be unmapped after the grace period. The Scan Auto-Unmapping page is found in Black Duck by clicking the Admin button → System Settings → Data Retention → Scan Auto-Unmapping.

New Automatic Scan Retry Header support for Black Duck Detect

A new Retry-After header has been added in the 429 response for Detect to know when to attempt a rate limited scan again. The following properties have been added to the `blackduck-config.env` file:

`BLACKDUCK_USE_QUEUE_RATE_LIMITING`: Set to `true` to enable queue base rate limiting in your environment. Default value is `false`.

`BLACKDUCK_INITIAL_RATE_LIMIT_DURATION_BRACKET_THRESHOLD_MINUTES`: dictates the duration the system must be rate limiting before the system moves from the first retry duration to the second retry duration.

`BLACKDUCK_RATE_LIMIT_DURATION_THRESHOLD_BRACKET_INCREMENT_MINUTES`: Dictates the duration that the system will stay in a rate limiting bracket before going to the next retry duration and multiplier.

`BLACKDUCK_INITIAL_RETRY_DURATION_MINUTES`: The initial duration of the Retry-After header in the first rate limiting bracket.

`BLACKDUCK_RETRY_DURATION_MULTIPLIER_MINUTES`: The amount to multiply the Retry-After Duration by each time the system reaches a new rate limit duration bracket.

New runtime threshold environment variable

You can now configure the threshold to determine long running jobs by adding the following variable to your `blackduck-config.env` file:

- `BLACKDUCK_DEFAULT_JOB_RUNTIME_THRESHOLD_HOURS`={value in hours}

The default value for this environment variable is 24 hours.

New Include Subprojects option for reports

You can now choose to include subprojects by checking the new **Include Subproject** checkbox in the report generation dialog box when creating the following reports:

- Notices File
- SBOM

- Version Details

Please note that this feature is enabled by default and subprojects were already included in report generation previous to this change. This feature now explicitly allows you to configure this functionality.

New Transitive Upgrade Guidance

Please note that this feature was added in Black Duck 2023.1.0 and was accidentally left out of the release notes for that version.

The simplest way to resolve security risk is to upgrade the version of the used component with fewer vulnerabilities. It is easier to do for components used as direct match. It is more difficult to mitigate or remove component vulnerabilities brought in as transitive dependencies without understanding what root direct dependency brought in that component. The goal of this feature is more simply and directly provide transitive upgrade guidance to provide a better developer experience and more clear call to action.

Enhanced Black Duck Secure Container (BDSC)

Black Duck introduces a new type of container image scan and project view to simplify managing the risk from container images. The container project can show the aggregated BOM and risk, but it also provides a way to view risk layer by layer, including separating risk from the base imagine or OS and the application layers. In addition, we've added support for viewing where and when components are added or removed in a layer.

Additionally, the Black Duck KnowledgeBase will expand its inventory to cover Docker Hub base container images and layer by layer component details to enable Black Duck to focus is scanning on the client container.

The existing Black Duck container image scanning as part of signature scanning, binary scanning, and Docker Inspector has not changed and will continue to be supported. The new container image scanning feature and project view will improve the user experience for managing risk found in containers enabling customers to manage the risk by container layer.

Please note that in order to take advantage of this feature, you must have Black Duck Secure Container (BDSC) enabled on your product registration key. Customers with a Black Duck Binary Analysis integrated subscription will have this included in their license.

Enhanced license risk aggregation - Limited customer availability

Prior to this enhancement, license risk from subprojects were not tracked or viewable within parent projects. This presented the possibility that license risk could be missed when using subproject hierarchies. Now, when you enable this feature, the License Risk displayed for a subproject in your project's BOM will be determined by the subproject's license risk and the highest license risk of its components.

Note that this feature is not general available and it not enabled by default. Enhanced license risk aggregation will be made generally available in an upcoming Black Duck release and will be enabled by default at that time.

Enhanced SBOM Import Component Visibility

You now have the ability to identify which components originated as a result of the SBOM import vs. other types of identification/scans or other imported SBOMs. In the Project Version's Source tab, you can identify the SBOM type (SPDX or CycloneDX), when the SBOM was imported, who supplied the SBOM, and the version of the tool used to create the SBOM.

Enhanced Component Versions page

The Component Versions page now more clearly displays what you are looking as far as security risk based on the scoring system priority set by System Administrator. The table now indicates if a component version has other vulnerabilities and how many that comes from another scoring system, such as CVSS v2.

Enhanced Jobs page functionality

The Processing tab of the Jobs pages will now display a warning icon next to jobs that are running longer than normal. You can also filter this page on Long Running jobs to display a list of these jobs.

In addition, new Prometheus metrics are available for users to see any jobs that are running longer than usual on the system.

Scanning hardware requirements changes

Black Duck 2023.10.0 sees a number of changes in scanning hardware requirements therefore Black Duck customers must update their environments and allocate additional hardware resources where necessary per the guidance below. Please see Black Duck Hardware Scaling Guidelines to stay up-to-date when changes are made to these recommendations.

Table 2: Hardware Scaling Guidelines

Name	Details	
10sph	**Scans/Hour**: 50 **SPH % Increase**: 400% **APIs/Hour**: 2,500 **Project Versions**: 10,000	**IOPS**: Read: 15,000 / Write: 9,000 **Black Duck Services**: CPU: 10 core / Memory: 36 GB **PostgreSQL**: CPU: 2 core / Memory: 8 GB **Total**: CPU: 12 core / Memory: 44 GB
120sph	**Scans/Hour**: 120 **SPH % Increase**: 0% **APIs/Hour**: 3,000 **Project Versions**: 13,000	**IOPS**: Read: 15,000 / Write: 15,000 **Black Duck Services**: CPU: 11 core / Memory: 56 GB **PostgreSQL**: CPU: 4 core / Memory: 16 GB **Total**: CPU: 15 core / Memory: 72 GB
250sph	**Scans/Hour**: 300 **SPH % Increase**: 20% **APIs/Hour**: 7,500 **Project Versions**: 15,000	**IOPS**: Read: 15,000 / Write: 15,000 **Black Duck Services**: CPU: 16 core / Memory: 85 GB **PostgreSQL**: CPU: 6 core / Memory: 24 GB **Total**: CPU: 22 core / Memory: 109 GB
500sph	**Scans/Hour**: 650 **SPH % Increase**: 30% **APIs/Hour**: 18,000 **Project Versions**: 18,000	**IOPS**: Read: 25,000 / Write: 25,000 **Black Duck Services**: CPU: 23 core / Memory: 133 GB **PostgreSQL**: CPU: 16 core / Memory: 64 GB **Total**: CPU: 39 core / Memory: 197 GB
1000sph	**Scans/Hour**: 1400 **SPH % Increase**: 40% **APIs/Hour**: 26,000 **Project Versions**: 25,000	**IOPS**: Read: 25,000 / Write: 25,000 **Black Duck Services**: CPU: 44 core / Memory: 367 GB **PostgreSQL**: CPU: 22 core / Memory: 88 GB **Total**: CPU: 66 core / Memory: 455 GB
1500sph	**Scans/Hour**: 1600 **SPH % Increase**: 6% **APIs/Hour**: 41,000 **Project Versions**: 28,000	**IOPS**: Read: 25,000 / Write: 25,000 **Black Duck Services**: CPU: 53 core / Memory: 464 GB **PostgreSQL**: CPU: 26 core / Memory: 104 GB **Total**: CPU: 79 core / Memory: 568 GB
2000sph	**Scans/Hour**: 2300 **SPH % Increase**: 15% **APIs/Hour**: 50,000	**IOPS**: Read: 30,000 / Write: 30,000 **Black Duck Services**: CPU: 64 core / Memory: 565 GB **PostgreSQL**: CPU: 32 core / Memory: 128 GB

Name	Details	
	Project Versions: 35,000	**Total**: CPU: 96 core / Memory: 693 GB

Table 3: PostgreSQL Settings

Name	Details	
10sph	**Scans/Hour**: 50 **PostgreSQL CPU/Memory**: 2 core / Memory: 8 GB `shared_buffers` (MB): 2654 `effective_cache_size` (MB): 3185	`autovacuum_max_workers`: 4 `maintenance_work_mem` (MB): 512 `max_connections`: 400 `work_mem` (MB): 50
120sph	**Scans/Hour**: 120 **PostgreSQL CPU/Memory**: CPU: 4 core / Memory: 16 GB `shared_buffers` (MB): 5336 `effective_cache_size` (MB): 6404	`autovacuum_max_workers`: 4 `maintenance_work_mem` (MB): 512 `max_connections`: 400 `work_mem` (MB): 50
250sph	**Scans/Hour**: 300 **PostgreSQL CPU/Memory**: CPU: 6 core / Memory: 24 GB `shared_buffers` (MB): 8016 `effective_cache_size` (MB): 9619	`autovacuum_max_workers`: 6 `maintenance_work_mem` (MB): 1024 `max_connections`: 500 `work_mem` (MB): 35
500sph	**Scans/Hour**: 650 **PostgreSQL CPU/Memory**: CPU: 16 core / Memory: 64 GB `shared_buffers` (MB): 21439 `effective_cache_size` (MB): 25727	`autovacuum_max_workers`: 6 `maintenance_work_mem` (MB): 1024 `max_connections`: 500 `work_mem` (MB): 35
1000sph	**Scans/Hour**: 1400 **PostgreSQL CPU/Memory**: CPU: 22 core / Memory: 88 GB `shared_buffers` (MB): 29502 `effective_cache_size` (MB): 35403	`autovacuum_max_workers`: 6 `maintenance_work_mem` (MB): 2048 `max_connections`: 600 `work_mem` (MB): 48
1500sph	**Scans/Hour**: 1600 **PostgreSQL CPU/Memory**: 26 core / Memory: 104 GB `shared_buffers` (MB): 34878 `effective_cache_size` (MB): 41854	`autovacuum_max_workers`: 8 `maintenance_work_mem` (MB): 4096 `max_connections`: 800 `work_mem` (MB): 58
2000sph	**Scans/Hour**: 2300 **PostgreSQL CPU/Memory**: 32 core / Memory: 128 GB `shared_buffers` (MB): 42974 `effective_cache_size` (MB): 51569	`autovacuum_max_workers`: 8 `maintenance_work_mem` (MB): 4096 `max_connections`: 800 `work_mem` (MB): 58

Updated policy evaluation of Archived project version phase

The following changes have been made to the Archived project version phase:

- The policy expression for project version phase no longer allows 'Archived' as a value.

- Existing policy rules that contain project version phase and 'Archived' value will be automatically disabled.
- New policy rules and expression changes will no longer be evaluated on project versions in 'Archived' phase.

Updated PostgreSQL settings

Starting with Black Duck 2023.10.0, PostgreSQL settings will be automatically set in deployments using the PostgreSQL container. Customers using external PostgreSQL will still need to apply the settings manually.

Updated Black Duck Hosted Detect version

Black Duck 2023.10.0 now offers support for Black Duck Detect 9 on the Black Duck Detect page and support for Detect 7.x has ended. After upgrading to Black Duck 2023.10.0, customers currently using Detect 7.x will see a warning indicator stating that Detect 7.x has reached end of support and that upgrading is recommended. Please note, you will not be able to revert to Detect 7.x after changing this configuration.

Updated Artifactory and SCM integrations requirements

In order to use the Artifactory and SCM integrations in your environment, you must have these features enabled on your registration key. Once enabled, you must add the following in your `values.yaml` file:

```
enableIntegration: true
```

Updated SCA as a Service deployment files

The deployment files used for SCA as a Service have been updated as follows:

- Updated RabbitMQ image from 1.2.14 to 1.2.29
- Added new environment variables in order to configure the ports to communicate correctly:
  - `BLACKDUCK_RABBIT_LISTENERS_PORT: "5672"`
  - `BLACKDUCK_RABBIT_MANAGEMENT_PORT: "15672"`

Updated Show Unmatched Components functionality

The `BLACKDUCK_HUB_SHOW_UNMATCHED` property used to determine whether or not "Unmatched Components" counts will be shown in project version components view is now enabled by default.

Please note this change was made in Black Duck 2023.7.0 and was inadvertently left out of that version's release notes.

Updated audit trails for SBOM fields

The Activity tab for a project will now report the addition or modification to the following SBOM fields:

- Package Supplier Name
- Package Supplier Email
- Package Supplier Type

Updated reporting database tables

The following tables have been updated:

- A `created_at` column has been added to the `component_policies` table. This column contains a list of times when policy violations were created.
- A `purl` column has been added to the `component` table. The column contains the package URL for the component.

Updated reporting database

The details stored as `channel_release_external_namespace` obtained via API is now available via the component table of the reporting database as well. It states the general namespace for the origin (maven, debian, ubuntu, etc).

Updated login page and frame

The login page and frame surrounding Black Duck has been updated.

Updated container scanning feature name

Black Duck Container Scanning - Limited Customer Availability has been renamed to Black Duck Secure Container (BDSC). Black Duck Secure Container scanning provides capabilities to identify components within container images, their layers and base images.

The Product Registration page has been updated accordingly.

Increased default storage service size on Kubernetes

Black Duck 2023.10.0 increases the container size and java heap size from 1GB storage / 512MB memory to 2GB storage / 1GB memory.

Container versions

- 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
- blackducksoftware/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 enhancements

Enhanced page navigation for REST API requests

REST APIs which returned paged results now provide links to other pages in the same sequence to help with iterating through the data.

Updated GET /api/jobs-runtimes request

We now include whether or not a job is long running in the `GET /api/jobs-runtimes` response.

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

The `longRunningThresholdMs` value determines the runtime threshold for the type of job. A job is considered long running if it exceeds this limit. The `longRunning` value determines whether or not the job is long running based on its runtime and the duration of previous job runs.

Improved performance for /api/project requests

Performance has been improved on the following API requests:

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

Binary scanner information

The binary scanner has been updated to version 2023.9.3.

- Now supports Container Scanning.

Fixed issues

The following customer-reported issues were fixed in this release:

- (HUB-27209). Fixed issue where KB Update Job could fail due to a vulnerability with no CVSS 2.0 score.
- (HUB-32753). Fixed an issue where upload cache cleaning did not handle outdated docker inspector uploads.
- (HUB-33560). The policy rule for the Archived project phase has been disabled. Any components that were in violation are cleared (even in archived project versions). New policy rules are NOT evaluated against 'archived' project versions. Expression changes are NOT evaluated against 'archived' project versions. Disabled and deleted policy rules - ARE cleared in 'archived' project versions.
- (HUB-35760). Fixed an issue where the Complete filter on the Scans page was incorrectly displaying scans currently in progress.
- (HUB-35836). Fixed an issue where users without any other direct access to a project could remove a project owner user and in doing so would assign the user without direct access as a project manager

role for the project. Users without direct access to a project will now be blocked from removing users from that project.

- (HUB-38385, HUB-38654). Fixed timeout issues related to the traditional method of processing scans.
- (HUB-38595). Updated the sample response for the `GET /api/codelocations/{codeLocationId}/latest-scan-summary` request in the REST API developer guide.
- (HUB-38682). Fixed an issue when clicking on the "N matches" link in the BOM view under Source column would not clear the previous selection in the Source tab and display the previously remembered matching folders/files.
- (HUB-38753). Fixed an issue where bulk edits of component version usage could incorrectly fail to update policy violations.
- (HUB-38766). Fixed an issue where project viewer users could access a project's settings page and make updates to the project. With this fix, Project Viewer users without permission will still be able to access the project settings page, but will now not be able to update anything. All update/delete actions will be disabled.
- (HUB-38803). Fixed an issue where snippets marked as ignored were still displayed when clicking the Unconfirmed Snippets link on the BOM page. Clicking this link will now automatically apply the Match Ignore: Not Ignored filter to the Snippets page.
- (HUB-38806). Fixed an issue where remediating the BDSA-2023-1225 via API vulnerability could generate a HTTP 404 error.
- (HUB-38841). Fixed the text size in the License notes and attribution statement of the Component License modal.
- (HUB-38878). Fixed an issue where a component could be deleted from BOM when a component merge occurred.
- (HUB-39079). Fixed an issue where trying to render large HTML reports could generate a HTTP 503 Service Unavailable server error response. Trying to render large HTML reports will now generate a validation error with the actual report size as well as the current limit. The current limit is determined by the `HUB_MAX_HTML_REPORT_SIZE_KB` environment variable which is set to 3000 KB by default.
- (HUB-39275). Fixed an issue where if the unmapped scan retention was set beyond 365 days in the UI, it would be reset it to 30 days when the purge job runs.
- (HUB-39318). Fixed an issue where it was not possible to highlight the origin in the Copyrights tab of a specific component's version.
- (HUB-39368). Fixed an issue when users would click on the other tabs, the global search was overriding the query for the currently selected search. Search requests will now not persist, meaning if a user refreshes the browser, or logs out and back in, previous filters will not be remembered.
- (HUB-39441). Fixed an issue with the ScmServerAppService where it would only check the scm integration registration key when initializing.
- (HUB-39496). Fixed an issue where BDIO generated from BDBA scans could fail to upload to Black Duck if the file size exceeded 16 GB. The limit has been increased to 90 GB.
- (HUB-39744). Fixed a discrepancy issue between the vulnerability results displayed on the BOM/versions page and the Dashboard after the KBUpdateWorkflowJob runs.
- (HUB-39836). Fixed an issue where the `component_matches` materialized view was not including all match types.
- (HUB-39864). Fixed an issue where editing a BOM component (changing usage or comment) with multiple origins (seen in hover over) could delete all origins.

- (HUB-40060). Fixed an issue when editing a component with many origins in a BOM, the selection was limited to 10 origins. This has been increased to 100.
- (HUB-40085). Fixed a performance issue with creating reports where generation could take much longer than expected, resulting in wait time in pipelines.

Black Duck SCA 2023.7.x

Black Duck version 2023.7.3

- Announcements
- New and changed features
  - API enhancements
  - Binary scanner information
  - Fixed issues

Announcements

Security Advisory for curl and libcurl (CVE-2023-38545, CVE-2023-38546)

Black Duck is aware of the security issue relating to curl and libcurl which was disclosed by the maintainer and original creator of the project on October 3, 2023.

CVE-2023-38545 impacts curl versions 7.69.0 through and including 8.3.0 and addresses a buffer overflow flaw that impacts both libcurl and the curl command line tool. The overflow can occur during a SOCKS5 handshake. If the handshake is slow, a user-supplied, unusually long hostname may not be resolved, and instead be copied into a target buffer for which it may exceed the allocated size. Heap-based buffer overflows such as these are known to lead to crashes, data corruption, and even arbitrary code execution.

CVE-2023-38546 is associated with a cookie injection flaw, but curl maintainers suggest that the series of conditions that must be met makes the likelihood of exploitation low. The versions impacted by this vulnerability are 7.9.1 through and including 8.3.0. Upgrading to curl 8.4.0 resolves the issue. Users are also advised to call curl_easy_setopt(cloned_curl, CURLOPT_COOKIELIST, "ALL"); after every call to curl_easy_duphandle();.

We believe that there is limited exposure to Black Duck' products, services and systems. To the extent we have had exposure, we have upgraded to the latest version of curl to remediate the situation.

For more information, please visit:

- Preparing for critical libcurl and curl vulnerabilities (CVE-2023-38545)
- How to respond to the curl and libcurl vulnerabilities

New and changed features

Container versions

NOTE: The nginx v2.0.61 and upload-cache v1.0.49 images were created specifically for 2023.7.3 to address the curl vulnerability and they should only be deployed with 2023.7.3. They are not compatible with Black Duck 2023.10.0.

- 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
- blackducksoftware/bdba-worker:2023.9.3
- blackducksoftware/rabbitmq:1.2.32

API enhancements

There are no new or changed API requests in Black Duck 2023.7.3. For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Binary scanner information

There are no changes to the binary scanner in 2023.7.3.

Fixed issues

The following customer-reported issues were fixed in this release:

- (HUB-40080). Fixed an issue where the refresh materialized view query for updating the `reporting.component_vulnerability` view could execute multiple times in parallel from multiple different ReportingDatabaseTransferJobs.

Black Duck version 2023.7.2

- Announcements
- New and changed features
  - API enhancements
  - Binary scanner information
  - Fixed issues

Announcements

There are no new announcements for Black Duck 2023.7.2.

New and changed features

There are no new or changed features in Black Duck 2023.7.2.

API enhancements

There are no new or changed API requests in Black Duck 2023.7.2. For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Binary scanner information

There are no changes to the binary scanner in 2023.7.2.

Fixed issues

The following customer-reported issues were fixed in this release:

- (HUB-39559). Fixed an issue where encryption key rotation was triggered incorrectly at every server start. Also, fixed an issue where the SAML private key was not included in the encryption key rotation.

Black Duck Version 2023.7.1

- Announcements
- New and changed features
  - API enhancements
  - Binary scanner information
  - Fixed issues

Announcements

Upcoming scanning hardware requirements changes

Black Duck 2023.10.0 will see a number of changes in scanning hardware requirements therefore Black Duck customers will need to update their environments and allocate additional hardware resources where necessary per the guidance below.

Table 4: Hardware Scaling Guidelines

Name	Details	
10sph	**Scans/Hour**: 50 **SPH % Increase**: 400% **APIs/Hour**: 2,500 **Project Versions**: 10,000	**IOPS**: Read: 15,000 / Write: 9,000 **Black Duck Services**: CPU: 10 core / Memory: 36 GB **PostgreSQL**: CPU: 2 core / Memory: 8 GB **Total**: CPU: 12 core / Memory: 44 GB
120sph	**Scans/Hour**: 120 **SPH % Increase**: 0% **APIs/Hour**: 3,000 **Project Versions**: 13,000	**IOPS**: Read: 15,000 / Write: 15,000 **Black Duck Services**: CPU: 11 core / Memory: 56 GB **PostgreSQL**: CPU: 4 core / Memory: 16 GB **Total**: CPU: 15 core / Memory: 72 GB
250sph	**Scans/Hour**: 300 **SPH % Increase**: 20% **APIs/Hour**: 7,500 **Project Versions**: 15,000	**IOPS**: Read: 15,000 / Write: 15,000 **Black Duck Services**: CPU: 16 core / Memory: 85 GB **PostgreSQL**: CPU: 6 core / Memory: 24 GB **Total**: CPU: 22 core / Memory: 109 GB
500sph	**Scans/Hour**: 650 **SPH % Increase**: 30%	**IOPS**: Read: 25,000 / Write: 25,000 **Black Duck Services**: CPU: 23 core / Memory: 133 GB

Name	Details	
	APIs/Hour: 18,000 **Project Versions**: 18,000	**PostgreSQL**: CPU: 16 core / Memory: 64 GB **Total**: CPU: 39 core / Memory: 197 GB
1000sph	**Scans/Hour**: 1400 **SPH % Increase**: 40% **APIs/Hour**: 26,000 **Project Versions**: 25,000	**IOPS**: Read: 25,000 / Write: 25,000 **Black Duck Services**: CPU: 44 core / Memory: 367 GB **PostgreSQL**: CPU: 22 core / Memory: 88 GB **Total**: CPU: 66 core / Memory: 455 GB
1500sph	**Scans/Hour**: 1600 **SPH % Increase**: 6% **APIs/Hour**: 41,000 **Project Versions**: 28,000	**IOPS**: Read: 25,000 / Write: 25,000 **Black Duck Services**: CPU: 53 core / Memory: 464 GB **PostgreSQL**: CPU: 26 core / Memory: 104 GB **Total**: CPU: 79 core / Memory: 568 GB
2000sph	**Scans/Hour**: 2300 **SPH % Increase**: 15% **APIs/Hour**: 50,000 **Project Versions**: 35,000	**IOPS**: Read: 30,000 / Write: 30,000 **Black Duck Services**: CPU: 64 core / Memory: 565 GB **PostgreSQL**: CPU: 32 core / Memory: 128 GB **Total**: CPU: 96 core / Memory: 693 GB

Table 5: PostgreSQL Settings

Name	Details	
10sph	**Scans/Hour**: 50 **PostgreSQL CPU/Memory**: 2 core / Memory: 8 GB `shared_buffers` (MB): 2654 `effective_cache_size` (MB): 3185	`autovacuum_max_workers`: 4 `maintenance_work_mem` (MB): 512 `max_connections`: 400 `work_mem` (MB): 50
120sph	**Scans/Hour**: 120 **PostgreSQL CPU/Memory**: CPU: 4 core / Memory: 16 GB `shared_buffers` (MB): 5336 `effective_cache_size` (MB): 6404	`autovacuum_max_workers`: 4 `maintenance_work_mem` (MB): 512 `max_connections`: 400 `work_mem` (MB): 50
250sph	**Scans/Hour**: 300 **PostgreSQL CPU/Memory**: CPU: 6 core / Memory: 24 GB `shared_buffers` (MB): 8016 `effective_cache_size` (MB): 9619	`autovacuum_max_workers`: 6 `maintenance_work_mem` (MB): 1024 `max_connections`: 500 `work_mem` (MB): 35
500sph	**Scans/Hour**: 650 **PostgreSQL CPU/Memory**: CPU: 16 core / Memory: 64 GB `shared_buffers` (MB): 21439 `effective_cache_size` (MB): 25727	`autovacuum_max_workers`: 6 `maintenance_work_mem` (MB): 1024 `max_connections`: 500 `work_mem` (MB): 35
1000sph	**Scans/Hour**: 1400 **PostgreSQL CPU/Memory**: CPU: 22 core / Memory: 88 GB `shared_buffers` (MB): 29502 `effective_cache_size` (MB): 35403	`autovacuum_max_workers`: 6 `maintenance_work_mem` (MB): 2048 `max_connections`: 600 `work_mem` (MB): 48
1500sph	**Scans/Hour**: 1600 **PostgreSQL CPU/Memory**: 26 core / Memory: 104 GB	`autovacuum_max_workers`: 8 `maintenance_work_mem` (MB): 4096 `max_connections`: 800

Name	Details	
	`shared_buffers` (MB): 34878 `effective_cache_size` (MB): 41854	`work_mem` (MB): 58
2000sph	**Scans/Hour**: 2300 **PostgreSQL CPU/Memory**: 32 core / Memory: 128 GB `shared_buffers` (MB): 42974 `effective_cache_size` (MB): 51569	`autovacuum_max_workers`: 8 `maintenance_work_mem` (MB): 4096 `max_connections`: 800 `work_mem` (MB): 58

New and changed features

New Artifactory configuration management

You can now manage your Artifactory Integration configurations within the Black Duck UI. To do so, log in as a Integration Manager user, click the Admin button, and then select Integrations.

As a result, a number of environment properties have been removed and are now configurable in the Black Duck UI. The following properties have been removed:

- `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`

New Docker image/container for Artifactory Integration service

A new Docker image/container has been added for use with Artifactory Integration. Hosted Black Duck customers must have Artifactory Integration enabled with their registration key before deploying this image/container.

New SCA Engine properties for Artifactory Integration

The following `environs` properties must now be added to Black Duck's `values.yaml` file in order for Black Duck and sca-engine-as-a-service to talk to each other:

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

NOTE: While these properties must be added to the `values.yaml` file, their values are not required to be set immediately and can be left blank as in the example above. The value of `BLACKDUCK_SCA_ENGINE_HOST` changes based on what you plan to name the sca-engine-as-a-service deployment.

New user roles

New user roles have been added to the list of overall roles:

- Integration Manager: This role grants the ability to manage all integrations.
- Lightweight BOM Code Scanner: This role grants administration privileges to a Lightweight BOM.
- Lightweight BOM Project Manager: This role grants administration privileges to a Lightweight BOM Project.
- Lightweight BOM Project Version Manager: This role grants administration privileges to a Lightweight BOM Project Version.

Updated full snippet scanning functionality

With increased usage of snippet scanning we are starting to see performance and scalability issues with snippet scanning. To help mitigate these issues, we are implementing tactical restrictions and optimizations to manage the throughput and reduce redundant re-work for snippet matching:

- Reduced the allowed range of maximum snippet file size to 1 - 4MB (from 1 - 16MB)
- Changed the default value of maximum snippet file size to 1MB (from 2MB)

In addition, full snippet scanning options must now be activated on your registration key. Affected Detect parameters are:

detect.blackduck.signature.scanner.snippet.matching

- `FULL_SNIPPET_MATCHING`
- `FULL_SNIPPET_MATCHING_ONLY`

Container versions

- 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
- blackducksoftware/bdba-worker:2023.6.0
- blackducksoftware/rabbitmq:1.2.28

API enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

New component metadata lookup via pURL API request

The following API request can be used to search a single component by using a package URL as search term. The response provides endpoints to fetch detailed information about the component, version and variant:

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

Updated components API endpoint response

The response of the following components API endpoint has been updated to include the `bomMatchInclusion` filter option (`true` or `false`) used in the request:

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

Binary scanner information

There are no changes to the binary scanner in 2023.7.1.

Fixed issues

The following customer-reported issues were fixed in this release:

- (HUB-38374). Fixed an issue with Black Duck SCM integration when using a different date/time format could cause an error when trying to pull repositories.
- (HUB-38790). Fixed issues with some migration scripts that were causing syntax errors.
- (HUB-38968). Fixed an issue where uploading a SBOM to Black Duck could fail due to the namespace UUID value not following SBOM best practices.
- (HUB-39026). Fixed an issue where the unmatched components badge, which is now enabled by default, would erroneously count package files when Detect 8 was run or when BDIO aggregation was

used. This caused the number of package managers run to be added to the unmatched component count due to the hierarchy in the BDIO file.

- (HUB-39072). Fixed the `CreatedAt` and `UpdatedAt` definitions for the BOM Component Vulnerability Remediation Representation in the REST API documentation to state that they are the date the vulnerability was added to the BOM component origin or updated on the BOM component origin.
- (HUB-39168). Fixed an UI issue where the "Add Filter" and "Filter versions..." text field options could disappear for modified components and the vulnerability history graph could disappear when a component is modified.
- (HUB-39211). Fixed an issue with the Japanese localization where the policy override date information was not being displayed correctly.
- (HUB-39274). Fixed an issue where the KbUpdateJob was not validating BDSA licensing from the customer's product registration which could cause a HTTP 403 Forbidden response during the request.
- (HUB-39367). Fixed an issue where license names containing "" could cause KbUpdateWorkflowJob-License Update to fail.

Black Duck version 2023.7.0

- Announcements
- New and changed features
  - API enhancements
  - Binary scanner information
  - Fixed issues

Announcements

End of support for Docker 18.09.x and 19.03.x.

Support for Docker 18.09.x and 19.03.x has ended in Black Duck 2023.7.0. Docker 20.10.x will be the only version supported.

Upcoming removal of gen02 sizing guidance

Black Duck 2023.10.0 will be removing gen02 sizing guidance and documents. Please refer to the Black Duck Hardware Scaling Guidelines page for sizing reference.

Upcoming end of support for PostgreSQL 13

With the upcoming 2023.10.0 release, Black Duck will end support for external PostgreSQL 13. Please refer to the Black Duck 2023.10.0. Please refer to the PostgreSQL Upgrade Schedule page for more information.

Upcoming PostgreSQL container migration to version 14

Black Duck will migrate its PostgreSQL image to version 14 with the 2023.10.0 release. Customers not using the Black Duck-supplied PostgreSQL image will not be affected.

Upcoming upgrade restrictions for PostgreSQL container users

Starting with 2023.10.0, Black Duck will only support direct upgrades from Black Duck versions that use the PostgreSQL 11 or PostgreSQL 13 containers (i.e., all Black Duck versions between 2022.2.0 and 2023.7.x inclusive). Users of the Black Duck-provided PG container upgrading from older Black Duck versions (i.e.,

all Black Duck versions prior to 2022.2.0) will require a 2-step upgrade: upgrade to 2023.7.x and then upgrade to 2023.10.x.

Documentation localization

The 2023.4.0 version of the UI, online help, and release notes have been localized to Japanese and Simplified Chinese.

New and changed features

PostgreSQL 15 support for external databases

Black Duck now supports and recommends PostgreSQL 15 for new installations that use external PostgreSQL. PostgreSQL 15 is not yet supported on Azure Database for PostgreSQL, therefore Black Duck recommends PostgreSQL 14 Flexible Server for users of that environment.

Migrating to Black Duck 2023.7.x does not require migration to PostgreSQL 15.

No action is required for users of the internal PostgreSQL container.

Encryption of report object types

Black Duck 2023.7.0 now marks report objects stored in the object store as sensitive, making them eligible to be encrypted at rest in the FILE volume where they are persisted. In order for them to be encrypted, Black Duck Crypto must be enabled in your environment with appropriate secrets provided. The following behavior changes will apply based on your environment's Black Duck Crypto setting:

For environments without Black Duck Crypto enabled at the time of upgrade to 2023.7.0

All existing reports and all new reports will remain unencrypted on disk - but marked as sensitive. If Black Duck Crypto is enabled later on, these objects will be encrypted in the background in order to comply with their sensitive nature.

For environments with Black Duck Crypto already enabled at the time of upgrade to 2023.7.0

If you have already enabled Black Duck Crypto, the existing reports will remain unencrypted and all new reports will be encrypted. If you need to force everything to be encrypted, set the environment variable `SYNOPSYS_CRYPTO_ROTATE_RESOURCES_ON_STARTUP=true` which will force the system to rotate the internal key and re-encrypt everything, including the old unencrypted reports.

Encryption for storage service objects

Sensitive objects stored in object storage FILE volumes will be encrypted at rest if Black Duck Crypto is enabled.

Updated Jobs page

The Jobs page has been redesigned to improve usability and scalabilty of the information displayed. The Jobs page has been broken down into three tabs:

- Finished: Displays all completed jobs, sucessful or failed.
- Scheduled: Displays all jobs scheduled to run in your environment.
- Processing: Displays all jobs currently in progress.

New Unmatched Origins management page

You can now more easily manage origin IDs that Black Duck identified during a package scan but could not be mapped to a component version. From the Unmatched Origins page, you can add or remove mappings to custom components which will then be added to subsequent package manager scans. The Unmatched Origins page can be reached by clicking Manage > Unmatched Origins.

In addition, you can now manage origin IDs mapped to custom components on their component version page.

Matching to custom components requires the use of Detect 7 or higher and is currently only supported for package manager scans.

Enhanced Notices File report

New options that can be added to the Notices File report:

- Deep License Data: Deep licenses discovered via component origin. Only available if deep licenses are enabled for the project.
- File Copyright Text: Copyright texts discovered in file matches. Only available if file matches are present.
- Unmatched File Discoveries: File discoveries unassociated with components in the project. Only available if unmatched files are present in the project.
- File License Data: Licenses discovered in file matches. Only available if file matches are present.

New SBOM report fields

The SPDX version of the SBOM report now includes two new optional fields:

- Package Comment: General comments about the package being described.
- Package Valid Until Date: The end of the support period for a package from the supplier.

You must first activate these fields under Manage > SBOM > BOM Component. Once enabled, you can update them by navigating to the project version's BOM, clicking the options button at the end of the component's row, and then selecting SBOM Fields.

Updated BOM filter label

The Match Status filter on the Component tab of the BOM project version page was ambiguously named. This filter only applies to snippet matches therefore the name was changed to Snippet Match Status to correctly capture that very specific use case.

Enhanced logging information

Added logging information (auth container) when a user logs in using username/password for both successful and failed logins.

Updated permission access for reports containing deleted projects

Access permission to reports have been updated where if one of the projects has been deleted, users can access if they have permission for all the remaining projects in the report (that haven't been deleted), or global project read access as part of their user role. Users not falling into either category above will not be able to access the report.

Enhanced Version Details report

The Version Details report now includes updates for sub-projects:

- The Version Details update guidance report now includes upgrade guidance for sub-projects.
- The first column of the project version update guidance report is now "Used by" which, if not blank, reports the subproject for the upgrade guidance.

Enhanced report generation

The mechanism for report data gathering and report format writing has been improved to constrain memory consumption. Please note that, as a result of this change, may result in longer report generation.

Consolidation of KnowledgeBase environment variables

Black Duck has a variety of environment variables to control KnowledgeBase scheme, host, and port configuration for a variety of KnowledgeBase services. Starting with Black Duck 2023.7.0, KnowledgeBase environment variable configurations have been unified on the following variables to simplify configuration:

- BLACKDUCK_KB_SCHEME
- BLACKDUCK_KB_HOST
- BLACKDUCK_KB_PORT

The following property prefixes have been explicitly removed and no longer referenced:

- BLACKDUCK_KBCLOUD
- BLACKDUCK_KBDETAIL
- BLACKDUCK_JSONWEBTOKEN

Users that have manually overridden old KnowledgeBase environment variables for customization should verify their environment to ensure functionality.

Updated date picker tool in UI

The date picker used in the UI has been updated which will change its appearance (depending on the browser) and functionality. Please note that, it does not get localized by the browsers language (except Firefox). It now depends on the operating systems locale for Chrome, Edge and Safari.

Supported browser versions

- Safari Version 16.4
  - Safari versions 14 and below are no longer supported
- Chrome Version 114.0.5735.198 (Official Build) (x86_64)
  - Chrome versions 91 and below are no longer supported
- Firefox Version 114.0.2 (64-bit)
  - Firefox versions 89 and below are no longer supported
- Microsoft Edge Version 114.0.1823.67 (Official build) (64-bit)
  - Microsoft Edge versions 91 and below are no longer supported

Container versions

- 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
- blackducksoftware/bdba-worker:2023.6.0
- blackducksoftware/rabbitmq:1.2.28

API enhancements

Removal of PUT /api/settings/data-retention

As mentioned in the 2023.4.0 release notes, `PUT /api/settings/data-retention` was deprecated in favor of `PATCH /api/settings/data-retention` and would return a HTTP 405 METHOD_NOT_ALLOWED error message when invoked. It has now been completely removed in Black Duck 2023.7.0 and will now return a HTTP 404 NOT_FOUND error message if used.

Deprecation of GET api/external-config/detect-uri

The `GET api/external-config/detect-uri` API request has been deprecated and replaced by `GET api/settings/detect`. Users can still use the old API while it is deprecated.

Authenticated users with no roles can still use `GET api/external-config/detect-uri` to get the API string while it is deprecated. If those users use the `GET api/settings/detect` API, they will get the detectUri (if it is set) and nothing else.

Improved performance for PUT /api/policy-rules/{policyRuleId}

Performance for the `PUT /api/policy-rules/{policyRuleId}` API request has been improved by limiting policy profile calculations to only run when a change in violation is found after evaluating components in a project version.

Updated POST api/components/{componentId}/versions

The `POST api/components/{componentId}/versions` API request has been updated to allow users to map an external ID to a new custom component version when created.

New public SBOM field endpoint

The `PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/sbom-fields` endpoint updates the saved values for sbom fields for a BOM component.

Binary scanner information

The binary scanner has been updated to version 2023.6.0.

- Now supports scanning package-lock.json files which may surfaces additional component identifications in comparison to previous scans. As a result, there may be an increase in components identified.

Fixed issues

The following customer-reported issues were fixed in this release:

- (HUB-21449). Fixed an issue with an incorrect policy violation display for vulnerability count in nested components when the violation was mitigated.
- (HUB-33362). Fixed an issue when trying to set up SAML with an XML file, the file would not save unless SAML is disabled.
- (HUB-34720). Fixed an issue when a license is modified, e.g. to reflect the original instead of the generic license text whilst not changing the license ID, the change was not exported to the SPDX file.
- (HUB-35512). Fixed an issue when adding a component version manually in the BOM page with a same component+version+origin, an "Unable to add manual BOM component because it already exists." error message will be consistantly displayed even if the origin setting is removed.
- (HUB-37067). Removed the Remediation Status filter from the Find → Vulnerabilities page.
- (HUB-37626). Fixed an issue where generating a SBOM report either on the UI or via API in JSON format for either v1.3 or v1.4 and attempting to retrieve it via `/api/projects/{projectId}/versions/{projectVersionId}/reports/{reportId}/contents` would display in a non-JSON format, including "/n" characters.
- (HUB-37763). Fixed an issue where the component counts API in license management did not match the linked "where used" counts results.
- (HUB-37796). Fixed an issue where MaaS could experience a scan failure with the error "Failed to create or update code location".
- (HUB-37922). Fixed an issue when attempting to use the bulk action feature on a BOM with more than 100 components specified.
- (HUB-38146). Fixed an issue where project version names containing the forward slash character (/) was causing the creation of subfolders in report generation. The forward slash character will now be substituted with the underscore character (_).
- (HUB-38347). Fixed an issue where the signature scan tool issue was not calculating the source code size properly when performing docker image inspector scans which could cause the scan to fail.
- (HUB-38480). Fixed an issue where the API request `/api/projects` always sorting by name, regardless of the sorting option used.
- (HUB-38535). Fixed an issue where the `/api/components/<component ID>/versions/<version ID>/licenses/<license ID>` API request does not return the correct license approval status after being changed.
- (HUB-38554). Fixed an issue when using the HUB UI to navigate KB component versions where it was forcing the pagination to be 25 regardless of entry specified by the user.
- (HUB-38587). Fixed an issue where the `kbMatchTimeoutProperty` was set inadvertantly to hardcoded value (100000ms) while the it should always read it from the blackduck-config.env file.
- (HUB-38590). Fixed an issue where the All origins dropdown of the Add Component dialog box was only displaying 10 rows which could cause some origins to not display.

- (HUB-38598). Fixed an issue where the Component Manager role could get a 403 Forbidden error when trying to access custom component versions after creation.
- (HUB-38646). Fixed an issue where private repositories where not visible via SCM integration. Note that you may have to delete the existing token from Black Duck for the changes to take effect.
- (HUB-38679). Renamed the Fulfillment Required column to Component Version Status in the Components report as it contains the component version's "Approval Status" to improve usability.
- (HUB-38685). Fixed an issue where project auto-delete was not using the new settings after being updated.
- (HUB-38720). Fixed an issue where the License text area was too small.
- (HUB-38774). Fixed an issue when attempting to unset the Release Date field within a project version would not persist, leaving the previously set date in place.

Black Duck SCA 2023.4.x

Black Duck version 2023.4.2

- Announcements
- New and changed features
  - API enhancements
  - Binary scanner information
  - Fixed issues

Announcements

There are no new announcements for Black Duck 2023.4.2.

New and changed features

There are no new or changed features in Black Duck 2023.4.2.

API enhancements

There are no new or changed API requests in Black Duck 2023.4.2. For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Binary scanner information

There are no changes to the binary scanner in Black Duck 2023.4.2.

Fixed issues

The following customer-reported issues were fixed in this release:

- (HUB-25500). Added mechanisms for users running on AWS to enable a workaround for this issue. Users experiencing this issue are encouraged to contact Black Duck support if they see high CPU usage from the upload-cache service. This issue will be fixed in the upcoming Black Duck 2023.10.0 release.
- (HUB-38587). Fixed an issue where the `kbMatchTimeoutProperty` was set inadvertantly to a hardcoded value (100000ms). It will now read it from the `blackduck-config.env` file as expected.
- (HUB-38735). Fixed an issue where upgrading from PostgreSQL 9.6 or PostgreSQL 11-based Black Duck versions to Black Duck 2023.4.1 could cause postgres-upgrader to fail and not start up the application when using the PostgreSQL container.

- (HUB-38815). Fixed an intermittent `ResourceAccessException` error in Black Duck rapid scans that could cause the scans to fail.

Black Duck version 2023.4.1

- Announcements
- New and changed features
  - API enhancements
  - Binary scanner information
  - Fixed issues

Announcements

Node constraints for storage and registration

With Black Duck 2023.4.1, users with multi-node swarm deployments are reminded to check the node constraints for storage and registration. This change will help alleviate the container shifting nodes and spreading data across multiple systems.

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

New and changed features

Improved unmatched file data purging

You can now purge unmatched file data for project versions that are specifically in the Archived project phase. This can be done globally through the Admin > System Settings > Data Retention page, which affects all projects, or locally for a selected project on its Settings page.

Note that the global setting only applies to projects and scans that do not explicitly specify their own setting; similarly, changing the global setting does not affect projects or scans that do specify their own setting.

SBOM report validation against policies

You can now configure specific project groups to validate the generation of SBOM reports against policies.

A new setting at the project group level (with project group access) can be enabled to prevent the generation of SBOM reports in projects that have any policy violations and provides the ability to apply the setting to projects in a group or all projects in all child groups.

When setting is enabled, when attempting to generate a SBOM report, you will be informed that the report can't be generated because the project has policy violations.

New SPDX v2.3 support for SBOM reports

You can now export the Software Bill of Materials report for your projects in SPDX v2.3 format.

New Project Alias SBOM field

A new optional Project Alias SBOM field has added to override project name and version info field at the project level. You must first activate the field under Manage > SBOM > Project. Once enabled, you can change the project's alias under the project's page > Settings.

API enhancements

Updated scan endpoints BDIO header information

The following API endpoints have been updated to use project and version names from the BDIO header instead of from HTTP headers:

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

Binary scanner information

Fixed issues

The following customer-reported issues were fixed in this release:

- (HUB-33736). Updated a number of API endpoints to use project and version names from the BDIO header instead of from HTTP headers. See the API enhancements section for more details.
- (HUB-36776). Fixed an issue where selecting 'Reveal in file tree' for a component in the Source tab did not show the file in the left side file tree for files part of the binary scan.
- (HUB-37280). Fixed an issue in SPDX 2.2 where all project files were listed despite "filesAnalyzed" being set to false.
- (HUB-38005). Removed the 'Vulnerability Reported' sorting option from the Find > Components page as it is no longer supported.
- (HUB-38141). Fixed a race condition when the scan client requested source files that did not belong to any matched directory/archive and were not stored in the database yet could cause inconsistent snippet scan results.
- (HUB-38212). Fixed an issue where a null pointer exception error could occur when importing a CycloneDX report.
- (HUB-38244). Fixed an issue where the Detect configuration page could display an error messsage when communicating with SIG Artifactory while running behind a proxy.
- (HUB-38279). Fixed an issue in the Black Duck UI under the 'Dashboard' tab where the 'Export Current View' button did not export the current view for 'Saved Searches'.
- (HUB-38312). Fixed an issue where vulnerability changes for bulk ignored components within Sub-Projects were not rolling up to the parent project.
- (HUB-38328). Fixed an issue where the policy override date info was not displayed correctly in Japanese settings due to an incorrect i18n character.

Black Duck version 2023.4.0

- Announcements
- New and changed features
  - API enhancements
  - Binary scanner information

- Fixed issues

Announcements

Upgrading to 2023.4.0 for Azure PostgreSQL users

If you are upgrading or installing using Azure PostgreSQL, a database administrator will need to enable installation of the `hstore` PostgreSQL extension before installing or upgrading to 2023.4.0 or later.

Moved pgcrypto extension into the st schema

Starting with Black Duck 2023.4.0, the pgcypto PostgreSQL extension is moved from the public schema into the `st` schema. If you are upgrading, using an external PostgreSQL instance, *and* the `blackduck` database user is not a superuser, you will need to relocate the extension manually with:

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

In all other cases, the move is performed automatically.

Removed MAX_CONCURRENT_JOBS from use in jobrunner

MAX_CONCURRENT_JOBS was deprecated in Black Duck 2022.10.x and has been removed in this release. Please refer to the Swarm and Kubernetes installation guides for assistance with configuring the newer mechanisms.

Deprecation of KBMATCH_SENDPATH in MaaS enabled systems

Match as a Service (MaaS) is now generally available with Black Duck 2023.4.0 and is enabled by default for new customers and will become standard for all existing customers. As a result of this update, the option to disable sending file path metadata to the KnowledgeBase for matching, `KBMATCH_SENDPATH`, is being removed in an upcoming Black Duck release.

Customers wanting to continue using this option will need to contact Black Duck support to have MaaS disabled for their Black Duck registration keys.

Upcoming end of support for Docker 18.09.x and 19.03.x

Starting with the 2023.7.0 release, Black Duck will no longer support Docker 18.09.x and 19.03.x. Docker 20.10.x will be the only version supported.

Upcoming end of life for Black Duckctl

Starting with the 2023.7.0 release, Black Duckctl will no longer be supported and there will be no more updates. Documentation for Black Duckctl can be found at https://github.com/blackducksoftware/hub/tree/master/kubernetes/blackduck.

Upcoming container scanning hardware requirements

With Black Duck 2023.10.0, the BDBA container will be required to perform container scanning. This means customers who currently perform container scans in Black Duck but do not have BDBA deployed with their Black Duck instance will need to allocate additional hardware resources per our guidance for the 2023.10.0 release to make use of the new container scanning functionality.

Existing functionality with container scanning will not be removed as part of this change.

Documentation localization

The 2023.1.0 version of the UI, online help, and release notes have been localized to Japanese and Simplified Chinese.

New and changed features

New SBOM upload functionality

The Scans page in Black Duck has been updated to separate the possible file types accepted when upload a report. When clicking the Upload File button, you can select from BDIO Scan, SBOM-SPDX, and SBOM-CycloneDX.

New BOM match score functionality

When we run signature scans, sometimes there is ambiguity in what we match. We might match a particular component and version, but there are multiple others that could match as well.

New in 2023.4.0, BOMs for your project versions will display a new column containing components' *match score*. The higher the match score, the more sure we can be that the matched component is in fact the component and version that we think.

You can configure how the match score thresholds are calculated in Admin > System Settings > Component Match Score. By configuring your match score thresholds, you can reduce ambiguous and low percentage matches, resulting in fewer false positives that will be displayed in your match results. Please note that configuring the thresholds too high might result in losing true positives in your match results.

As a result of improvements made with the new match ambiguity logic, you might see different results when viewing your BOMs.

New centralized Black Duck Detect hosting and version management

Black Duck now offers a new means to connect with Black Duck Detect to better suit your needs; Black Duck Hosted. This method works best with non-airgapped customers who want Blackduck to manage the version of Detect to use. In system settings, Black Duck will provide a dropdown list of major Detect versions and their latest exact versions from which you can select to perform your scans.

New Artifactory Integration functionality

Black Duck 2023.4.0 now allows Kubernetes users using JFrog Artifactory to do both Binary and Docker Image/Container scans on their artifacts, extending the signature scan supported in the earlier phase. Currently, we support two deployment options: Full on-premise and Hybrid. Please see the Kubernetes install guide for deployment requirements and instructions.

New scan rate limiting on all scan ingress endpoints

Based on heap memory, if the scan container uses more than 80% of the available allocated heap (`HUB_MAX_MEMORY`), it waits until the heap usage reaches 60% before allowing scans through again. The container will also allow one scan through every 300 seconds per (which is the default value of `blackduck.scan.ingress.scanPassThroughIntervalSecs`), even if the rate limiting is enabled and active.

New Black Duck storage container

Added in Black Duck 2023.1.0, a new storage service was introduced which enables you to move static files, such as SBOMs and other reports, to persistent storage, which frees up the database and enables scan performance and scalability enhancements.

NOTE: This item was accidentally left out of the Black Duck 2023.1.0 release notes.

New configuration of custom volumes for Blackduck Storage

Starting in 2023.4.0, the storage container may be configured to use up to three (3) volumes for the storage of file based objects. In addition, the configuration can be set up to migrate objects from one volume to another. The backup scripts `hub_create_data_dump.sh` and `hub_db_migrate.sh` have been updated to save the file provider volume accordingly.

New filtering support for heatmaps

You can now filter the data displayed in the heatmap. Filtering options include code location ID, code location name, project name, scan data, scan status, scan type, and version name.

Enhanced Rapid Scan results data for BOM support

You can now configure Rapid Scan to provide a full results format to include data points for BOM support. To do so, set the following environment variable: `BLACKDUCK_RAPID_SCAN_EXTENDED_DATA=true`. The new data points include:

- componentDescription
- Homepage link
- OpenHub link
- Declared License definition
- Release date
- Meta links to component id, component version id and component version origin URIs
- External namespace
- Package URL
- SPDX license ID
- Source (NVD or BDSA)
- Match type

Enhanced policy violation management

You can now set an expiration date for policy overrides on the Black Duck BOM page. By clicking the violation icon for a component, you can enter a date until which the policy violation is overridden. When it expires it will return to a violation state.

Enhanced dependency tree view

You can now highlight needed information in the Dependency Tree view in order to copy/paste it.

Removed CentOS download link for Detect Desktop

The Tools page has been updated to remove the CentOS download link for Detect Desktop as it is no longer supported for Black Duck.

Preliminary support for PostgreSQL 15

Black Duck 2023.4.0 adds preliminary support for using PostgreSQL 15 as an external database. This support is for *testing only*; production use IS NOT SUPPORTED.

Supported browser versions

- Safari Version 16.3 (17614.3.7.1.7, 17614)
  - Safari versions 13.1 and below are no longer supported
- Chrome Version 111.0.5563.146 (Official Build) (x86_64)

    - Chrome versions 79 and below are no longer supported
- Firefox Version 111.0.1 (64-bit)
    - Firefox versions 74 and below are no longer supported
- Microsoft Edge Version 111.0.1661.62 (Official build) (64-bit)
    - Microsoft Edge versions 79 and below are no longer supported

Container versions

- 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
- blackducksoftware/bdba-worker:2023.3.0
- blackducksoftware/rabbitmq:1.2.21

API enhancements

Updated components endpoints

The following public API endpoints have been updated to allow the updating of component, version and origin id.

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

New JobHistoryAppService API endpoints

Two new public REST API endpoints have been added which uses the JobRuntimeRepository to get information about job runtimes and provide information about them:

- `/api/jobs-histories`

- `/api/jobs-histories-filters`

New JobRuntimeAppService API endpoint

Two new public REST API endpoints have been added which uses the JobRuntimeRepository to get information about job runtimes and provide information about them:

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

Please note that you should use the `/api/job-runtimes` endpoint to view running jobs. The existing `/api/jobs` endpoint will be deprecated in favor of the new endpoint.

New JobScheduleAppService API endpoint

Three new public REST API endpoints have been added which outputs a list of jobs that are scheduled on the system.

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

Please note that you should use the `/api/job-schedules` endpoint to view scheduled jobs. The existing `/api/jobs` endpoint will be deprecated in favor of the new endpoint.

New JobRunner API endpoint

A new public REST API endpoint has been added which allow users to enable/disable periodic jobs. Please note that changing settings in this way can cause unexpected behavior on your system.

- `/api/jobs-schedules-configurations`

New centralized Detect version management API endpoints

The following endpoints have been added to support the new centralized Detect version management functionality offered in Black Duck 2023.4.0:

- `GET /api/settings/detect`
  - Gets the current detect version management settings
  - If accessed by an authenticated non-system administrator user, they will only receive `detectUri` (if it has a value)
  - If accessed by an authenticated system administrator user, they will receive the following information:
    - `detectUri`: The Detect URI saved by a system administrator.
    - `useInternalHosting`: Boolean, determines the type of hosting used for Detect (internally hosted or Black Duck hosted). Returns false if not using an internally hosted version of Detect.
    - `useMajorVersion`: Boolean, determines if the latest of a major version of Detect is used. Returns true if "Latest 8.x" or "Latest 7.x" was selected in UI.
    - `selectedVersion`: String, returns the version of Detect used.
    - `allowDowngrade`: Boolean, notifies if the system setting allows the user use an older version of Detect.

    - `majorVersions`: String, the list of current valid major versions of Detect.
    - `allVersions`: String, the list of all current valid versions of detect.
- `PATCH /api/settings/detect`
    - Updates the detect version management settings
    - Requires authenticated access by a system administrator user
    - Updates the following information:
        - `detectUri`: Internal Detect URI.
        - `useInternalHosting`: Boolean, sets the type of hosting used for Detect (internally hosted or Black Duck hosted).
        - `useMajorVersion`: Boolean, sets the latest major version or an explicit version of Detect. Updated and required if `useInternalHosting` is false.
        - `selectedVersion`: String, the Detect version to use, either a major version or exact version. Only updated if `useInternalHosting` is false.
        - `allowDowngrade`: Boolean, if managed, allows earlier versions of Detect to be used.

Deprecation of PUT /api/settings/data-retention

As mentioned in the 2022.10.0 release notes, `PUT /api/settings/data-retention` has been deprecated and replaced with `PATCH /api/settings/data-retention`. In Black Duck 2023.4.0, `PUT /api/settings/data-retention` will now return a HTTP 405 METHOD_NOT_ALLOWED error message.

Binary scanner information

The binary scanner has been updated to version 2023.3.0.

.

Fixed issues

The following customer-reported issues were fixed in this release:

- (HUB-32471). Fixed an issue when scans had KnowledgeBase connectivity issues, it was not reported in the UI and resulted in an empty BOM.
- (HUB-33018). Fixed an issue where vertical and horizontal scrollbars could appear when printing a BOM.
- (HUB-34474). Fixed an issue where filtering projects would not display correctly when project names have full-width uppercase letters.
- (HUB-34616). Fixed an issue where the jobs listed on the Diagnostics page did not display milliseconds for completed jobs.
- (HUB-34964). Fixed issue where vulnerability "used by" count on the find page was inconsistent with the vulnerability affected projects page.
- (HUB-34981). Fixed an issue where the "used by" count on the component version list view was inconsistent with the component version details view.
- (HUB-35075). Fixed a display issue when trying to Save to PDF the BOM page in the Chrome browser.
- (HUB-35092, HUB-35171, HUB-36088). Fixed an issue where adding or deleting a component to a project/version in the Archived phase using the API request would result in a 200 OK response, but the

component was not actually added or deleted. Now, an error will be displayed if this is attempted. The UI will also no longer display a Delete option.

- (HUB-35773, HUB-37305). Fixed an issue where, as a result of binary scan, in the Source tab of a BOM, a single file matched to more than one component would only display one of the components.
- (HUB-35836). Fixed an issue when removing a project owner from a project, Black Duck was not preventing the project from becoming orphaned. A direct access User assignment check has now been added to prevent this action from being performed.
- (HUB-36108). Fixed an issue where snippet scanning was facing long running and timeout issues due to QuartzSnippetScanAutoBomJob.
- (HUB-36351). Fixed the API documentation regaring Updating a Custom Component Version and Creating a Custom Component Version.
- (HUB-36387). Fixed a concurrency issue in remediation status update where mitigating particular vulnerabilities via API would allow the mitigation to be applied, but the riskPriorityDistribution does not reflect all the mitigations.
- (HUB-36446). Fixed an issue where downloading the Sigma tool could fail with an HTTP 401 unauthorized message.
- (HUB-36676). Fixed a file permission issue when trying to install Platform One Black Duck on OpenShift environments.
- (HUB-36716). Fixed an issue where BDSA auto-remediated vulnerabilities do not get removed from being displayed on ignored components in new project versions or clones.
- (HUB-36719). Fixed an issue when adding a subproject to a parent project, unchecking the "Include in Notices File Report" checkbox would include the subject in the notice report regardless. Unchecking this checkbox for a subject will now exclude the subproject from all projects above in the project hierarchy.
- (HUB-36763). Fixed an issue where the SigmaToolStoreStateCheckAndRetryJob could fail due to the user's configured proxy. The job should no longer fail in the case where access to sig-repo is unreachable when not using a proxy, but reachable when using it.
- (HUB-36905). Fixed an issue where signature scanning a single leaf file could cause a null pointer exception error.
- (HUB-36952). Fixed null pointer exception in file and package adjustment operations.
- (HUB-37031). Fixed an issue with match count discrepencies and missing URI property from matched-files response when MaaS is enabled.
- (HUB-37078). Fixed issues on multiple UI pages where the back button in the browser could take multiple tries for function to work.
- (HUB-37109). Removed the ability to set the usage on snippet matches as it is currently not supported in the product. It remains available for all other match types.
- (HUB-37232). Fixed an issue where auto scroll sometimes did not work when opening discoveries with source code upload for: License, License Reference, Copyright.
- (HUB-37233). Fixed a REST API documentation issue where the "BOM component representations" link in the description of "The specific sub-set of BOM component representations requested" would go to "BOM Component Version Representation" instead of "BOM Component Representation".
- (HUB-37308). Fixed an issue where the scan size in the list of Scans page would include snippet scan size, incorrectly displaying the sum of both totals.

- (HUB-37312). Fixed an issue where a "Unable to access tool" error could be generated if the `/opt/blackduck/hub/uploads/tools` directory doesn't exist in the mounted storage volume when looking for objects.
- (HUB-37414). Fixed an issue where the Scans status on Project BOM page could get stuck in processing state and only refreshing the page would update the status.
- (HUB-37439). Fixed an issue where the length of the path matched by the snippet is very long, the path will not be fully displayed on the snippet view.
- (HUB-37453). Fixed an issue where applying any filter to the project versions page would not persist after refreshing or navigating away from the page.
- (HUB-37505). Fixed an issue with the ordering of jobs on the Jobs page (/api/jobs) was incorrect. The jobs will now be listed by end time descending.
- (HUB-37554). Fixed an issue when using the `/api/projects/<id>/versions/<id>/components/<id>/versions/<id>` API request with the parameters `component` and `componentVersion` missing could cause an error. To set a component to have an unknown version, set the componentVersion field to the empty string "".
- (HUB-37648). Fixed an issue with binary scans (with BDBA integrated) where the Source tab and Source report would only shows a single component match for each binary file even if the Components tab and Component report shows multiple components.
- (HUB-37661). Fixed an issue when BOM references another project, the Security tab could display blank loading areas.
- (HUB-37696). Fixed an issue where comment containing URLs for components would not word wrap correctly, causing it to go offscreen. Due to the security reasons, links will be displayed as plain text. Users would need to copy paste to navigate to them.
- (HUB-37757). Fixed an issue the Delete button on the Scans page could stop working after being used due to the page not refreshing as expected after use.
- (HUB-37775). Fixed an issue when trying to manually add the component origin using the edit option, the full path of the origin ID would not being displayed completely.
- (HUB-37789). Fixed an issue where it was no longer possible to copy the name of the match file/folder from source tree view.
- (HUB-37925). Fixed an issue where after filtering projects by an option on Summary tab, it was not possible to remove the filter via UI.

Black Duck SCA 2023.1.x

Black Duck version 2023.1.2

- Announcements
- New and changed features
  - API enhancements
  - Binary scanner information
  - Fixed issues

Announcements

Updated automatic project version deletion feature

Black Duck 2023.1.0 updated the automatic project version deletion feature (formerly known as Automatic Data Removal). This feature is now enabled by default upon upgrading to 2023.1.0 and any upcoming future releases.

Automatic project version deletion allows the automatic removal of old project versions within Black Duck. The default settings will remove project versions which have not been updated or scanned within 90 days. Upon upgrading to 2023.1.x, any old project versions which have not been updated or re-scanned in 45 days will be deleted 45 days after upgrade assuming they are not re-scanned or updated post upgrade. These settings can be changed under the system administrator data retention settings page.

New and changed features

New automatic OAuth Token refresh

Black Duck will now automatically regenerate GitLab and Bitbucket access tokens after they expire.

Enhanced heatmap functionality

Scans in the "Started" state will now be included in the heatmap UI metrics.

API enhancements

There are no new or changed API requests in Black Duck 2023.1.2. For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Binary scanner information

There are no new or changed features for the binary scanner in Black Duck 2023.1.2.

Fixed issues

The following customer-reported issues were fixed in this release:

- (HUB-35747). Fixed issue that would block certain periodic jobs (`BomAggregatePurgeOrphansJob`, `KbUpdateWorkflowJob`) from finishing.
- (HUB-36781). Fixed an issue where versions of Black Duck 2022.10.x could not be installed with custom fsGroup on Kubernetes or OpenShift.
- (HUB-36796). Fixed an issue where having a user directly assigned to a Project Group and the same user assigned to a User Group that's also assigned to the Project Group would result in multiple project groups being returned by the API, resulting in a Detect failure.
- (HUB-36939). Fixed an issue where the debug page exposed the password in plain text if the user logged into Black Duck as the sysadmin.
- (HUB-36997). Fixed an issue where license information was missing for notice files generated using KnowledgeBase on-prem.
- (HUB-37143). Fixed an issue where rapid scans that evaluate the policy expression 'Newer Versions Count' fail with internal error if the component does not have a version.
- (HUB-37285). Fixed an issue where new installations of Black Duck 2023.1.0 using an external database could fail if the default admin user name was changed.

- (HUB-37312). Fixed an issue where a `Unable to access tool` error could be generated if the `/opt/blackduck/hub/uploads/tools` directory doesn't exist in the mounted storage volume when looking for objects.

Black Duck version 2023.1.1

- Announcements
- New and changed features
  - API enhancements
  - Binary scanner information
  - Fixed issues

Announcements

There are no new announcements for Black Duck 2023.1.1.

New and changed features

There are no new or changed features in Black Duck 2023.1.1.

API Enhancements

There are no new or changed API requests in Black Duck 2023.1.1. For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Binary scanner information

The binary scanner has been updated to version 2022.12.0 which includes a new retry policy and fixes to improve network communication resiliency with Black Duck to accomodate the expansion of scan capacity resource limiting to ensure the reliability of integrated binary scans.

Fixed issues

The following issue was fixed in this release:

- (HUB-37171). Fixed an issue where the authentication container could fail to come online when crypto is enabled.

Black Duck version 2023.1.0

- Announcements
- New and changed features
  - API enhancements
  - Binary scanner information
  - Fixed issues

Announcements

Increased system resource requirement for object storage service

The minimum system resource requirements to deploy the object storage service has increased for Black Duck 2023.1.0. The object storage service will require approximately an additional 1 cpu, 1GB of memory, and 10GB of disk space. Please note that these requirements will change again in future releases.

Database object ownership change

Database objects (e.g., tables, views, etc.) owned by blackduck (or the user-specified alternate, if provided) have had their ownership changed to blackduck_user (or the user-specified alternate, if provided).

End of support for Helm2

Black Duck no longer supports Helm2 for Kubernetes deployments. The minimum supported version of Kubernetes has increased to 1.13 (the oldest version supported by Helm3).

Documentation localization

The 2022.10.0 version of the UI, online help, and release notes have been localized to Japanese and Simplified Chinese.

New and changed features

Updated SCM integration - Phase 3

Black Duck 2023.1.0 has added two new SCM providers to the list of SCM integrations:

- GitLab Self-Managed
- Bitbucket Data Center

You can now add these authorized SCM providers which can then be selected when creating a new project. Doing so will automatically pre-populate the repository URL and branch version in the Project Settings page for your new project.

This feature is compatible with Detect 8.x and above, and will take effect with new package manager scans.

Please note that SCM integration is not enabled by default in Black Duck and must be activated by adding the following in your environment:

For Swarm users, add the following to your `blackduck-config.env` file:

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

For Kubernetes users, add the following to your `values.yaml` file under the environs section:

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

Updated project version auto-deletion

Project version auto-deletion, formely known as automatic data removal, is now managed in the Black Duck user interface. To do so, click Admin > System Settings > Data Retention.

Enhanced analysis and aggregation of file sizes during signature scan processing

Overly large scans will no longer take down the match engine service, instead it will fail the scan with an error saying the *calculated* size is greater than the registered limit. The calculated size is either:

- The full size of the scan if it is within the registration limit.
- The last calculated size of the scan just after it exceeds the registration limit. Calculation of scan size will not contunue if it has already exceeded the licensed limit.

Stateless signature scan (formerly Ephemeral Signature Scan)

The Stateless Scan is a new scan mode that does not create or use any permanent storage within Black Duck, thus there is no bill of material (BOM) stored. It is used to quickly find policy violations within the designated scan target. In order to use Stateless Scan, you must have the following:

• Black Duck Detect 8.2.0 or later

• Black Duck 2022.10.0 or later

• Hosted KnowledgeBase

• Match as a Service must be enabled

Added support for Docker Swarm secrets encryption

Black Duck has added support for Docker Swarm secrets encryption to centrally manage data such as passwords, SSH private keys, SSL certificates, or other pieces of data and securely transmit it to only those containers that need access to it.

Added application level encryption and key rotation

Starting in version 2023.1.0, Blackduck supports encryption of critical data, such as Git SCM OAuth tokens, Git app secret, SAML private signing keys, and LDAP credentials, within the system. This encryption is based upon a secret provisioned to the Blackduck installation by the orchestration environment (Docker Swarm or Kubernetes).

New Component Insights page

Certain components found in scans may have additional details useful in determining extra information for a component's origin. The Component Insights page gives you better understanding about how components are operating and what functionality is offered. If the component has additional insights, you can view it by going to the project version's page, and selecting Insights in the options menu for that component.

New SBOM report fields for project groups

You can now add new additional SBOM fields to your project groups to include more detail to your software bill of materials (SBOM) reports:

- **Creator**: The person(s) or organization(s) that created the SPDX file inlcuding email addresses.
- **Creator Comments**: An optional field for creators of the SPDX file to provide general comments about the creation of the SPDX file or any other relevant comment not included in the other fields.

New KB license update and security update jobs

The current KB Update job will be split into KB Security Update job and KB License Update job. The KB License Update job is scheduled to run daily by default and can be configured to change the frequency of the job, as well as to allow you to disable the job if needed using the following system properties:

- `KB_LICENSE_UPDATER_PERIOD_MINUTES`: Sets the job frequency in minutes.
- `KB_UPDATE_JOB_ENABLED`: Set to false to disable both the security and license update jobs.

Updated referenceLocator URLs in SBOM reports

The `referenceLocator` field in SBOM reports will now only display the Black Duck KB unique ID instead of the URL.

Enhanced Rapid Scan functionality

Black Duck 2021.10.0 introduced project groups defined policy rules so that customers can scope policy rules by specific project groups which could only be used in Full Scan mode. New in Black Duck 2023.1.0, project group based policies are now supported in Rapid Scan mode.

Rapid Scan users can specify the scanned project's parent project group using the following Detect parameter:

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

- The project group name must match exactly to an existing project group on Black Duck.
- If the <project group name> is provided and the project does not exist in Black Duck, it will be used as the project group for policy determination.

Updated v3 signature scan failure handling

Starting in 2023.1.0, all v3 signature scans that would exceed the code location limit or the total scanned code limit will fail on create instead of after ingress. Failures will not be displayed in the Black Duck UI, but on the scan client instead.

Improved performance related to searching

Searches in Black Duck use materialized views in the database that are refreshed at regular intervals to allow for faster search results. The refresh of these views, however, was causing problems with large databases. We analyzed all of the filters and determined that some were not needed. From the various search categories, we removed the following filters:

Project Version Search

- Distribution
- Tier

Component Search

- Policy Rule
- Policy Violation Severity
- Component Approval Status
- Review Status
- Vulnerability Reported
- Vulnerability CWE

Vulnerability Search

- Base Score
- Exploitability Subscore
- Impact Subscore
- Temporal Subscore
- Reachable

Saved searches will be updated via migration script to remove those filters. Bookmarked search results will still function. However, removed filters will be ignored, so the results will be as if the filter was never selected. Saved searches comprised exclusively of removed filters will be removed entirely.

New scan heatmap

You can now view an on demand heatmap which displays the total number of scans performed on a given day and hour over the last 30 days. The color coded matrix displays the total number of scans based on a minimum/maximum relationship, with green values signifying lower values and red values signifying higher values. The heatmap can be found in Black Duck by clicking the Admin button and then selecting Heatmaps in the Diagnostics section.

New Black Duck storage container

Black Duck 2023.1.0 introduces a new storage service which enables you to move static files, such as SBOMs and other reports, to persistent storage, which frees up the database and enables scan performance and scalability enhancements.

Reporting schema change

In Black Duck 2023.1.0, the type of the `basedir` column in `reporting.scan_view` has been changed from character varying to text to accommodate paths longer than 255 characters.

New Project Group Administrator role

The new Project Group Administrator role has the ability to manage project groups on a local level. For example, they are able to create/edit/delete project groups and add/remove members and user groups from project groups below their parent project group.

Supported browser versions

- Safari Version 16.2 (17614.3.7.1.7, 17614)
  - Safari versions 13.0 and below are no longer supported
- Chrome Version 109.0.5414.87 (Official Build) (x86_64)
  - Chrome versions 71 and below are no longer supported
- Firefox Version 109.0 (64-bit)
  - Firefox versions 71 and below are no longer supported
- Microsoft Edge Version 109.0.1518.55 (Official build) (64-bit)
  - Microsoft Edge versions 78 and below are no longer supported

Container versions

- 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
- blackducksoftware/bdba-worker:2022.12.0
- blackducksoftware/rabbitmq:1.2.15

API Enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Enhanced project endpoints

The following endpoints have been updated to include OSS component pURL coordinates:

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

Updated data-retention API endpoint

The following endpoint has been changed from a PUT to a PATCH request:

- `/api/settings/data-retention`

New tool list API endpoint

A new public endpoint is now available to list all available tool versions:

- `/api/tools`

New fetch for SBOM fields for specific project group

A new public endpoint is now available to read a project's SBOM fields:

- `/api/project-groups/{projectGroupId}/sbom-fields`

Binary scanner information

The binary scanner has been updated to version 2022.12.0 which includes a new retry policy and fixes to improve network communication resiliency with Black Duck to accomodate the expansion of scan capacity resource limiting to ensure the reliability of integrated binary scans.

Fixed issues

The following customer-reported issues were fixed in this release:

- (HUB-32387). Fixed an issue where redis could not access /data on default Openshift environments.

- (HUB-33820). Fixed an issue where a warning could appear after a component was updated in the BOM (e.g. its status in the KnowledgeBase is set to "reviewed") but would not disappear until the user reloaded the page manually.
- (HUB-34056). Fixed an issue where individual component edit displayed different results from bulk component edit when "Adjust Snippets and Confirm" was checked at the Edit dialog.
- (HUB-34374). Fixed an issue where the value in Discovery Types column on the source tab of the project version page could display inconsistently with filters.
- (HUB-34502). Fixed an issue where confirmed/unconfirmed snippet results were not included in the source report when including ignored components in reports.
- (HUB-34596). Fixed an issue where a duplicate constraint error would occur when attempting to create a SAML user sharing the same username as the internal user.
- (HUB-34725). Fixed an issue with duplicated `FILE_DEPENDENCY_DIRECT` and `FILE_DEPENDENCY_TRANSITIVE` entries in version reports.
- (HUB-34756). Fixed an issue where the scope showing as 'Server' when user group roles assigned through project groups using the API.
- (HUB-34947). Fixed an issue where ignored snippets could be displayed in SPDX reports.
- (HUB-35472). Fixed an issue where changing the value of `MAX_TOTAL_SOURCE_SIZE_MB` did not apply correctly in synopsysctl.
- (HUB-35557). Fixed an issue where improperly formed /api/projects/ requests would return a HTTP 5xx error code instead of a HTTP 4xx error code.
- (HUB-35585). Fixed an issue where the "Updated By" data was not updated and always reflecting "System Administrator" as the username of the user who made the change and has the old date/time.
- (HUB-35764). Fixed some GUI bugs in the top menu and in the snippet window.
- (HUB-35912). Fixed an issue where confirmed and then ignored snippet matches would disappear when the license risk filter with all the options selected was applied.
- (HUB-35914). Fixed an incorrect flag in the the system_check.sh script (using -z instead of -n).
- (HUB-35927). Fixed an issue where the remediation status and comment was not reverted by the Auto-Remediation feature if there are change in CVE BDSA mapping for components.
- (HUB-35945). Fixed an issue where the Scan Size value on the Project Version's Scans page did not include the size value of code locations as displayed on the main Scans page.
- (HUB-36321). Fixed an issue where the Edit option in the Source view for snippets was available to the Project Viewer role.
- (HUB-36382). Fixed a rare race condition generating an error when receiving more than one scan in rapid succession.
- (HUB-36498). Fixed an issue where the GET /api/vulnerabilities/<CVE RECORD>/affected-projects could return a HTTP 400 error code if the CVE had too many records.
- (HUB-36629). Fixed an issue where Rapid Scans could report extra vulnerabilities violating a policy rule.
- (HUB-36703). Fixed an issue where the Match type in the Black Duck UI and `/api/projects/{projectId}/versions/{projectVersionId}/matched-files` API request were different. See the API enhancements section above for details.
- (HUB-36707). Fixed an issue where Rapid Scan could timeout instead of end in error quickly if the project or version name was misspelled.

Black Duck SCA 2022.10.x

Black Duck version 2022.10.3

- Announcements
- New and changed features
  - API enhancements
  - Binary scanner information
  - Fixed issues

Announcements

There are no new announcements for Black Duck 2022.10.3.

New and changed features

There are no new or changed features in Black Duck 2022.10.3.

API Enhancements

There are no new or changed API requests in Black Duck 2022.10.3. For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Binary scanner information

The binary scanner has been updated to version 2022.9.2 which includes an upgrade to OpenSSL 3.0.7 in response to the high severity CVE-2022-3602 and CVE-2022-3786 vulnerabilities.

Fixed issues

The following issue was fixed in this release:

- (HUB-37171). Fixed an issue where the authentication container could fail to come online when crypto is enabled.

Black Duck version 2022.10.2

Announcements

There are no new announcements for Black Duck 2022.10.2.

New and changed features

There are no new or changed features in Black Duck 2022.10.2.

Container versions

- 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
- blackducksoftware/bdba-worker:2022.9.2
- blackducksoftware/rabbitmq:1.2.14

API Enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Enhanced project endpoints

The following endpoints have been updated to include OSS component pURL coordinates:

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

Binary scanner information

The binary scanner has been updated to version 2022.9.2 which includes an upgrade to OpenSSL 3.0.7 in response to the high severity CVE-2022-3602 and CVE-2022-3786 vulnerabilities.

Fixed issues

The following customer-reported issues were fixed in this release:

- (HUB-35377). Fixed an issue where unconfirmed snippets and ignored component were showing up in component or license usage counts anywhere within Black Duck except the source view when reviewing unconfirmed/ignored snippets.
- (HUB-35850). Fixed an issue where Redis could not access data on default Openshift environments.
- (HUB-36049). Fixed an issue where `FileBackedOutputStream` temp files were written to `/tmp` directory under the scan container and are not cleaned up.
- (HUB-36149). Fixed an issue when printing a BOM as a PDF, it did not include the project name and version name.
- (HUB-36359). Fixed the missing link to the `blackduck-webui` container on the Guthub release page.
- (HUB-36495). Fixed some outdated images the online help.

Black Duck version 2022.10.1

Announcements

Security Advisory for OpenSSL versions 3.0.0 to 3.0.6

On November 1, 2022, the OpenSSL Project disclosed the following high severity vulnerabilities present in OpenSSL 3.0.x.

The nature of both vulnerabilities allows a buffer overrun which can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer.

CVE-2022-3602: An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution.

CVE-2022-3786: An attacker can craft a malicious email address in a certificate to overflow an arbitrary number of bytes containing the `.' character (decimal 46) on the stack. This buffer overflow could result in a crash (causing a denial of service).

Currently, Black Duck believes there is limited exposure to Black Duck SIG products, services, and systems. To the extent we have had exposure, we have applied mitigations that prevent attempted exploitation.

The binary scanner (BDBA) has been updated to version 2022.9.2 which includes an upgrade to OpenSSL 3.0.7 in response to the high severity vulnerabilities. Customers running 2022.10.0 without BDBA do not need to upgrade.

Please continue monitoring our Community page for further updates.

New and changed features

There are no new or changed features in Black Duck 2022.10.1.

Container versions

- 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
- blackducksoftware/bdba-worker:2022.9.2
- blackducksoftware/rabbitmq:1.2.14

API Enhancements

There are no new or changed API requests in Black Duck 2022.10.1. For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Binary scanner information

The binary scanner has been updated to version 2022.9.2 which includes an upgrade to OpenSSL 3.0.7 in response to the high severity CVE-2022-3602 and CVE-2022-3786 vulnerabilities.

Fixed issues

The following customer-reported issues were fixed in this release:

- (HUB-36290). Updated BDBA worker in response to the OpenSSL vulnerabilities.

Black Duck version 2022.10.0

Announcements for 2022.10.0

PostgreSQL 11 deprecation

Support for running Black Duck on PostgreSQL 11 has ended with the 2022.10.0 release. Starting with this release, attempting to run Black Duck with PostgreSQL 11 will generate an error and Black Duck will fail to start.

PostgreSQL 13 container migration

Black Duck 2022.10.0 has migrated its PostgreSQL image from version 11 to version 13 and supports upgrading from versions using either the PostgreSQL 9.6 container (versions 4.2 through and including 2021.10.x) or the PostgreSQL 11 container (versions 2022.2.0 through and including 2022.7.x). During installation, the `blackduck-postgres-upgrader` container will migrate the existing database to PostgreSQL 13 and then exit upon completion.

Customers with non-core PG extensions are STRONGLY encouraged to uninstall them before migrating and reinstall them after the migration completes successfully; otherwise, the migration is likely to fail.

Customers with replication set up will need to follow the instructions in the pg_upgrade documentation BEFORE they migrate. If the preparations described there are not made, the migration will likely succeed, but the replication setup will break.

Customers not using the Black Duck-supplied PostgreSQL image will not be affected.

IMPORTANT: Before starting the migration:

- Ensure that you have an extra 10% disk space to avoid unexpected issues arising from disk usage due to the data copying of system catalogs.
- Review root directory space and volume mounts to avoid running out of disk space as this can cause Linux system disruptions.

For Kubernetes and OpenShift users:

- On plain Kubernetes, the container of the upgrade job will run as root. However, the only requirement is that the job runs as the same UID as the owner of the PostgreSQL data volume.

- On OpenShift, the upgrade job assumes that it will run with the same UID as the owner of the PostgreSQL data volume.

For Swarm users:

- The migration is completely automatic; no extra actions are needed beyond those for a standard Black Duck upgrade.
- The `blackduck-postgres-upgrader` container MUST run as root in order to make the layout and UID changes described above.
- On subsequent Black Duck restarts, `blackduck-postgres-upgrader` will determine that no migration is needed and immediately exit.

Database bds_hub_report deprecation

As stated in the release notes for Black Duck 2021.10.0, new installations of Black Duck will no longer create the `bds_hub_report` database. We will be deleting the `bds_hub_report` database in 2022.10.0.

Users wishing to save their `bds_hub_report` database can use the `hub_create_data_dump.sh` script to dump the `bds_hub_report` database if it exists.

Notice of Black Duck KnowledgeBase IP Address Change Nov 2022

During the week of November 14th 2022 the Black Duck KnowledgeBase https://kb.blackducksoftware.com IP address will be changing. During the week of the 14th, we will be updating the DNS to direct traffic to the new IP addresses. For most customers, no action is required.

On-prem customers who use IP allow listing to communicate to the KB will need to update their firewall, allow lists to include these new IP address. Customers who do not use firewall rules to restrict traffic or IP allow listing will not be affected.

For customers who use IP address, allow listing will need to add the following IP addresses:

NAM (North America)

kb-na.blackducksoftware.com : 34.160.126.173

EMEA (Europe, Middle East and Africa)

kb-emea.blackducksoftware.com: 34.149.112.69

APAC (Asia Pacific, Asia and China)

kb-apac.blackducksoftware.com: 34.111.46.24

This change will not affect the majority of customers which use DNS resolution, as this will automatically handle the IP address update. Customers who are use IP address whitelisting will need to add the three new IP address to their whitelist: 34.160.126.173, 34.149.112.69, 34.111.46.24.

The current IP address are included below for reference only:

NAM: 35.224.73.200

EMEA: 35.242.234.51

APAC: 35.220.236.106

We are making this change as part of our continued efforts to deliver a highly available and secure KB.

Please submit a support case if there are questions or problems after the server migration.

Upcoming system resource requirement for object storage service

The minimum system resource requirements to deploy the object storage service will increase in Black Duck 2023.1.0. The object storage service will require approximately an additional 1 cpu, 1GB of memory, and 10GB of disk space. Please note that these requirements will change again in future releases.

Documentation localization

The 2022.7.0 version of the UI, online help, and release notes have been localized to Japanese and Simplified Chinese.

New and changed features in 2022.10.0

Git repository SCM integration - Phase 2

Black Duck 2022.10.0 has updated the way users can add repository/branch fields when creating a project and version. You now have the ability to add authorized SCM providers (GitHub Standard and GitHub Enterprise only at this time) which can then be selected when creating a new project. Doing so will automatically pre-populate the repository URL and branch version in the Project Settings page for your new project.

This feature is compatible with Detect 8.x and above, and will take effect with new package manager scans.

Please note that SCM integration is not enabled by default in Black Duck and must be activated by adding the following in your environment:

For Swarm users, add the following to your `blackduck-config.env` file:

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

For Kubernetes users, add the following to your `values.yaml` file under the environs section:

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

New bulk actions for project version components

The bulk update feature now supports the following actions on components on the project versions page:

1. Ignore/unignore components
2. Set component usage type
3. Mark as reviewed/unreviewed
4. Set include/exclude in notices file

Creating reports using UTF8 with BOM

Please note that this feature was added in Black Duck 2022.7.0 and was accidentally omited from that version's release notes.

Black Duck 2022.7.0 introduced support for UTF8 with BOM character encoding in reports for customers using non-Western characters. To enable this feature, add the following to the `blackduck-config.env` file:

```
USE_CSV_BOM=true
```

New heatmap data download

You can now review and analyze terminal scan trends by downloading the heatmap as a compressed CSV and create the heatmap as a pivot in a spreadsheet program. This data can be downloaded by navigating to **Admin** > **Diagnostics** > **System Information**.

New SBOM report fields

You can now add new additional SBOM fields to your projects to include more detail to your software bill of materials (SBOM) reports. SBOM fields include the following new fields.

Set on the BOM component level:

- Package URL: Listed in the `externalRefs` section as `referenceType: purl` for `referenceCategory: PACKAGE_MANAGER` elements in SPDX reports, and under the `components` section as `purl` for CycloneDX reports.
- Package Supplier: Listed as (`supplier`) for both report types.
- CPE: Listed in the `externalRefs` section as `referenceLocator` for `referenceCategory: SECURITY` elements in SPDX reports, and under the `components` section as `cpe` for CycloneDX reports.

Set on the component level:

- Description: Listed as `description` for both report types.
- Originator: Listed as `originator` under the `packages` section for SPDX reports, and as `author` under the `components` CycloneDX reports.

New Global Notification Viewer role

A new role has been created that has read only access to all projects and receives all system notifications regardless of user preferences.

New notification subscription management

You now have the ability to enable or disable which notifications your users receive. You can manage these settings by going to **Admin** > **System Settings** > **Notifications**. Please note that users with the Global Notification Viewer role will still receive all notifications on the system.

Updated notifications management for watched projects

You can now manage which watched projects you receive notifications from in your My Settings page. To do so, click your user name on the top right menu, click Watched Projects, and then select the Watched Projects tab.

Updated notification retention period

The default configuration value for notification retention has been reduced to 14 days from 30. This can be modified by setting the `BLACKDUCK_HUB_NOTIFICATIONS_DELETE_DAYS` variable in `blackduck-config.env`.

New vulnerability conditions for policies

A new Vulnerability Tags category has been added to the Vulnerability Conditions of policies replacing and including the Remote Code Execution (RCE) vulnerability. This category includes the following filter options when creating or editing policies:

- **Zero-click Remote Code Execution**: Vulnerabilities which can result in the execution of code on the system, triggered by a remote attacker without requiring or relying on any third party action.
- **Malicious Code Identified**: Software containing code with malicious intent and is designed to have harmful or destructive consequences if executed within your system.
- **Embargoed Vulnerability Details**: Vulnerabilities whose technical details are currently under embargo and the details are not published by the vendor at this time.
- **Unconfirmed Vulnerability**: Vulnerabilities that do not have a code-based fix because the vendor has decided that the behavior of the component is intended and does not believe there is a vulnerability.

New vulerability tags added to Vulnerablity Update reports

Vulnerability Update reports will now display vulnerability tags where applicable. These include the Vulnerability tags listed above.

New export functionality for lists and tables

You can now export lists and tables to CSV on the following pages:

- Dashboard page: Found in the Results Summary section of the Dashboard.
- Find page: Found above the search field on the left side of the Find page.
- Scans page: Found next to the delete button on the top left side of the Scans page.
- Users & Groups page: Found next to the Create User button on the top left side of the Users & Groups page.

Enhanced source view when importing BDIO for binary scanning and Protex BOM imports

Currently, the Scans page lists the *Components Not Found* in the BOM Import Log. Now with the 2022.10.0 release, unmatched components will also be surfaced in the Source View tab. Please note that unmatched components will be surfaced in the Source view for new scans only. Existing scans will be unchanged.

Reporting schema enhancements

The `reporting.component` view now has three additional fields:

- `reporting.component.created_at`: The created at time for the component, copied from the BOM. Represents the first time the component was added to the BOM.
- `reporting.component.updated_at`: The updated at time for the component, copied from the BOM. Represents the most recent time that component was updated in it's BOM.
- `reporting.user_group_project_mapping`: Adds which user is mapped to which group/groups and which user is mapped to which project/projects.

New Ephemeral Signature Scan - Limited customer availability

The Ephemeral Signature Scan is a new scan mode that does not create or use any permanent storage within Black Duck, thus there is no bill of material (BOM) stored. It is used to quickly find policy violations within the designated scan target. In order to use the Ephemeral Signature Scan, you must have the following:

- Black Duck Detect 8.2.0 or later
- Black Duck 2022.10.0 or later
- Hosted KnowledgeBase

- Match as a Service must be enabled

Please note that this feature is limited customer availability and is not generally available in Black Duck 2022.10.0.

Updated synopsysctl

Black Duckctl has been updated to work with the new PostgreSQL 13 container.

Container versions

- 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
- blackducksoftware/bdba-worker:2022.9.1
- blackducksoftware/rabbitmq:1.2.14

API enhancements

For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

New scan monitoring API endpoint

A new REST API endpoint has been added which analyzes scan error rates and allows you to get the scan monitoring information from terminal scans in the system in a given time frame (default is set to the last hour):

- `GET /api/scan-monitor`

Request parameters are as follows:

- `level` (*mandatory*). Number value `1` or `2`, default is `1`.
  Example request: `GET /api/scan-monitor?level=1`

  Level `1` is a simple binary response, either `OK` or `NOT OK` if the failure rate exceeds the set maximum threshold amount (default is 30%).

Level 2 returns a hex color code (green, yellow, or red) depending on the status. Green (`#00FF00`) indicates that the failure rate in the monitored timeframe (default is the last hour) is less than the set minimum threshold amount (default is 10%). Yellow (`#FFFF00`) indicates that the failure rate is between the minimum and maximum thresholds (10% and 30%). Red (`#FF0000`) indicates that the failure rate is greater than the maximum threshold amount (30%).

Enhanced handling of null values for custom fields

The following public API requests have been updated to return an error message if the custom field values are null:

- `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}`

Updated notification endpoints

The following REST API public endpoints have been updated to return the `notifyUser` field based on whether the user should receive notifications for the subscription:

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

New BOM status endpoint

A new REST API endpoint has been created to determine when a BOM has been updated for a given scan:

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

Possible status values are `NOT_INCLUDED`, `BUILDING`, `SUCCESS`, `FAILURE`.

Deprecation of PUT /api/settings/auto-remediate-unmapped

In Black Duck 2022.4.1, the public endpoint `PUT /api/settings/auto-remediate-unmapped` was changed to `PATCH /api/settings/auto-remediate-unmapped` but the `PUT` endpoint was deprecated and kept in order to maintain backward supportability. As of this release, the `PUT /api/settings/auto-remediate-unmapped` endpoint is now deleted.

Deprecation and removal of licenses API requests

The following API requests have been removed:

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

As a result of the removal of `GET api/licenses/{licenseId}/obligations`, the obligation API will no longer be returned by any APIs. The license term API (`/api/licenses/{licenseId}/license-terms`) will be returned instead.

In addition, the following API requests have been deprecated:

- `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`

New and enhanced component endpoints

A new REST API endpoint has been added to get/modify SBOM field values on component level:

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

The following REST API endpoint has been enhanced to get SBOM field values for a component which includes `sbom-field` endpoint in meta/links section :

- `GET /api/components/{componentId}`

New PATCH /api/settings/data-retention endpoint

The new `PATCH /api/settings/data-retention` REST API endpoint will replace the existing `PUT /api/settings/data-retention`. As a result, `PUT /api/settings/data-retention` has been deprecated and will be removed in an upcoming release.

New Dependency Upgrade Guidance public API endpoint

A new REST API endpoint has been added to provide data for Dependency Upgrade Guidance:

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

Updated /api/projects/{projectId}/versions/{projectVersionId}/matched-files endpoint

The `/api/projects/{projectId}/versions/{projectVersionId}/matched-files` endpoint now includes a "matchTypeFilterValue" flag to better handle inconsistency when viewing the results. The following table displays how `matchType` is mapped to `matchTypeFilterValue`:

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

Binary scanner information

The binary scanner has been updated to version: 2022.9.1. The binary scanner now includes support for NPM through package manager support.

Fixed issues in 2022.10.0

The following customer-reported issues were fixed in this release:

- (HUB-29825). Fixed an issue where assigning the Global Security Manager to both Personal and Group overall Roles does not allow for remediate (grayed out) when the System Setting "Project Manager Role Settings > Security Manager" is disabled.
- (HUB-30488). Fixed an issue where the hierarchal BOM Tree could intermittently not show children components (Tree would not trickle down).
- (HUB-33274). Updated the REST API documentation to include "componentVersionName" and "componentVersion" for "BOM Component Representation".
- (HUB-33407). Fixed an issue where some users would receive a "You've exceeded your maximum amount of code you can scan" notification when they have unlimited codebase size.
- (HUB-33693). Fixed an issue where the uploaded source window in Snippet View might not display immediately.
- (HUB-33847). Fixed an issue when the clone categories field `cloneCategories` is not present in the body of a project creation request, all clone categories will be selected/enabled. In addition, when creating a project via the API the field `projectLevelAdjustments` defaults to 'true' when it is not present.
- (HUB-33922). Fixed an issue where only 7 days worth of job history was displaying in Admin > Diagnostics > Jobs when it should have been 30 days worth.
- (HUB-33945, HUB-34938). Fixed an issue where generating large HTML Vulnerability Reports in Black Duck for a project was crashing the application or taking much longer than expected. As part of the fix, we added a configurable `HUB_MAX_HTML_REPORT_SIZE_KB` property to manage HTML report downloads. This property will only affect HTML report viewing, not generation or downloading of any other report.
- (HUB-33972). Fixed an issue where string search/copyright search might not work with the OnPrem KB March data.
- (HUB-34085). Fixed an issue where sorting by name on the component management page was case sensitive.
- (HUB-34246). Fixed browser display issues related to the Project Version Comparison view.
- (HUB-34511). Fixed an issue where the project name of dependency scan could become unreadable characters when using Chinese characters.
- (HUB-34676). Fixed an issue where updating disabled custom fields could trigger BOM computation across all project versions.
- (HUB-34712). Fixed an issue where binary scan pods could get into a CrashLoopBackOff state due to the health check timeout settings for BDBA containers being out of sync with docker swarm

and kubernetes (30 seconds). Also, the health check timeout is now customizable so that it can be customized:

- For Kubernetes, use the following argument where ### is the value in seconds: `--set binaryscanner.timeout=###`
- For Docker Swarm, provide the timeout value in the docker stack deploy command where ### is the value in seconds:

```
BDBA_HEALTH_CHECK_TIMEOUT=### docker stack deploy -c docker-compose.yml -c sizes-gen03/10sph.yaml -c docker-compose.bdba.yml hub
```

- (HUB-34839). Added a postgres-upgrader section to `docker-compose.local-overrides.yml`.
- (HUB-34887). Fixed an issue for air-gapped environments where the phone-home call could hang for a long time, causing the system to misbehave when the registration service was unresponsive.
- (HUB-35110). Fixed the documentation inside `blackduck-config.env` for the default retention period of unmapped code locations.
- (HUB-35140). Fixed an issue where the comments on components with shared vulnerabilities comments were not origin-specific.
- (HUB-35184). Upgraded Zulu Java version to 11.0.16+8 to remediate vulnerabilities found in Black Duck 2022.4.2.
- (HUB-35196). Fixed an issue where using the Component/Component Version filter did not show Component name results.
- (HUB-35222). Fixed an issue where the "Affected projects" tab was not able to load pages when navigating through them for a specific vulnerability (CVE-2016-1000027).
- (HUB-35366). Fixed an issue where custom field values were not appearing in Component details screen.
- (HUB-35369). Fixed an issue when printing the Black Duck BOM pdf, the report would overlap at the edge of pages and would not list all the components correctly.
- (HUB-35407). Fixed an issue where custom fields with null values could cause the KbUpdateWorkflowJob-Component Version Update job to fail.
- (HUB-35524). Fixed user permissions issues when using the `/api/projects/<project_id>/versions/<version_id>/policy-rules` public endpoint.
- (HUB-35660). Fixed an issue with duplicate entry ids in the scan client which could cause an exit Code 70 - "java.util.ConcurrentModificationException" error.

Black Duck SCA 2022.7.x

Announcements for Version 2022.7.2

There are no new announcements for Black Duck 2022.7.2.

New and changed features in version 2022.7.2

There are no new or changed features in Black Duck 2022.7.2.

Container versions

- 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
- blackducksoftware/bdba-worker:2022.6.0
- blackducksoftware/rabbitmq:1.2.10

API Enhancements

There are no new or changed API requests in Black Duck 2022.7.2. For more information on API requests, please refer to the REST API Developers Guide available in Black Duck.

Fixed Issues in 2022.7.2

The following customer-reported issues were fixed in this release:

- (HUB-35687). Fixed an issue when a CVE and BDSA vulnerability are related and the related vulnerability could be incorrectly added to a vulnerability remediation. If this occurs, the `vulnerable-bom-components` API would return a HTTP Response 400 / Bad Request error when applied to a component with this issue.

Announcements for Version 2022.7.1

There are no new announcements for Black Duck 2022.7.1.

New and changed features in version 2022.7.1

Git repository SCM integration - Phase 2

Black Duck 2022.7.1 has updated the way users can add repository/branch fields when creating a project and version. You now have the ability to add authorized SCM providers (GitHub Standard and GitHub Enterprise only at this time) which can then be selected when creating a new project. Doing so will automatically pre-populate the repository URL and branch version in the Project Settings page for your new project.

This feature is compatible with Detect 8.x and above, and will take effect with new scans.

Please note that SCM integration is not enabled by default in Black Duck and must be activated by adding the following in your environment:

For Swarm users, add the following to your `blackduck-config.env` file:

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

For Kubernetes users, add the following to your `values.yaml` file under the `environs` section:

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

New heatmap data download

You now have the ability to download the heatmap data which holds information for terminal scans in the system. You can download this information by going to **Administration** > **Diagnostics** > **System Information**. From there, click the **Download Heatmap (.zip)** button. The output is a `.csv` file.

Creating reports using UTF8 with BOM

Please note that this feature was added in Black Duck 2022.7.0 and was accidentally omited from that version's release notes.

Black Duck 2022.7.0 introduced support for UTF8 with BOM character encoding in reports for customers using non-Western characters. To enable this feature, add the following to the `blackduck-config.env` file:

```
USE_CSV_BOM=true
```

New bulk actions for project version components

The bulk update feature now supports the following actions on components on the project versions page:

- Ignore/unignore components
- Set component usage type
- Set include/exclude in notices file

Container versions

- 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
- blackducksoftware/bdba-worker:2022.6.0
- blackducksoftware/rabbitmq:1.2.13

API Enhancements

For more details on new or changed API requests, please refer to the API doc available in Black Duck.

New scan monitoring API endpoint

A new REST API endpoint has been added which analyzes scan error rates and allows you to get the scan monitoring information from terminal scans in the system in a given time frame (default is set to the last hour):

- `GET /api/scan-monitor`

Request parameters are as follows:

- `level` (*mandatory*). Number value 1 or 2 or 3, default is '1'.
  Example request: `GET /api/scan-monitor?level=1`

  Level 1 is a simple binary response, either `OK` or `NOT OK` if the failure rate exceeds the set maximum threshold amount (default is 30%).

  Level 2 returns a hex color code (green, yellow, or red) depending on the status. Green (#00FF00) indicates that the failure rate in the monitored timeframe (default is the last hour) is less than the set minimum threshold amount (default is 10%). Yellow (#FFFF00) indicates that the failure rate is between the minimum and maximum thresholds (10% and 30%). Red (#FF0000) indicates that the failure rate is greater than the maximum threshold amount (30%).

  Level 3 returns aggregated scan counts based on scan states.

  The monitored timeframe, minimum, and maximum thresholds can all be configured in the `blackduck-config.env` file for your environment.

Enhanced handling of null values for custom fields

The following public API requests have been updated to return an error message if the custom field values are null:

- `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}`

Fixed Issues in 2022.7.1

The following customer-reported issues were fixed in this release:

- (HUB-33693). Fixed an issue where the scanned file view of a file with snippets would not load unless the panel was clicked.
- (HUB-34246). Fixed browser display issues when printing the Project Version Comparison view.
- (HUB-34472, HUB-34781, HUB-34682). Fixed an issue where removing licenses on the Component Version page not reflect in the BOM report.
- (HUB-34511). Fixed an issue where project and version names were pulled from HTTP headers instead of the BDIO header which could cause unreadable characters when using non-latin characters.
- (HUB-34618). Improved the performance when generating the Version Detail report on KB On-prem environments.
- (HUB-35110). Fixed the documentation inside `blackduck-config.env` for the default retention period of unmapped code locations.
- (HUB-35196). Fixed an issue where using the Component/Component Version filter did not show Component name results.
- (HUB-35222). Fixed an issue where the "Affected projects" tab was not able to load pages when navigating through them for a specific vulnerability (CVE-2016-1000027).
- (HUB-35304). Fixed an issue where the super user role assigned to a user group was not migrated to the new roles introduced in 2022.7.0 when upgrading to 2022.7.0.
- (HUB-35349). Fixed an issue where Rapid Scans scans could fail after upgrading to Black Duck 2022.7.0 due to messages being sent after the matching process was finished. It was more likely to occur when the environment had multiple match containers running.
- (HUB-35407). Fixed an issue where custom fields with null values could cause the KbUpdateWorkflowJob-Component Version Update job to fail.

Announcements for Version 2022.7.0

PostgreSQL 9.6 deprecation

As previously announced, support for running Black Duck on PostgreSQL 9.6 ended with the 2021.6.0 release of Black Duck. Starting with the 2022.7.0 release of Black Duck, attempting to run Black Duck with PostgreSQL 9.6 will generate an error, and Black Duck will fail to start.

Upcoming PostgreSQL 11 deprecation

Support for running Black Duck on PostgreSQL 11 will end with the 2022.10.0 release. Starting with that release, attempting to run Black Duck with PostgreSQL 11 will generate an error and Black Duck will fail to start.

PostgreSQL container migration from 11 to 13

Black Duck will migrate its PostgreSQL image from version 11 to version 13 with the **2022.10.0** release. Customers not using the Black Duck-supplied PostgreSQL image will not be affected.

Upcoming custom-fields API change

In the 2023.1.0 release of Black Duck, the following APIs will change to return errors when trying to read or change a custom field that is disabled. The field will need to be re-enabled before it can be accessed.

- `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}`

Support for legacy signature scans and legacy package manager scans deprecation

This functionality will be officially sunset in the Black Duck 2023.7.0 release.

Customers should upgrade to Detect 8.x to ensure compatibility. Detect 8.x is tentatively targeted for release in May/June 2022 which aligns with Black Duck 2022.7.0 release and this deprecation release note. This will give customers a one year period to upgrade Detect in alignment to the future sunset date.

Upcoming Helm2 end of support

Starting with the 2023.1.0 release, Black Duck will no longer support Helm2 for Kubernetes deployments. The minimum supported version of Kubernetes will increase to 1.13 (the oldest version supported by Helm3).

Correction: Git repository SCM Integration - Phase 1

Instructions provided in the 2022.4.0 release notes regarding enabling Git repository SCM Integration in Black Duck for Swarm users were incorrect. The correct variable setup is as follows:

For your `docker-compose.yaml` webapp environment:

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

Also, in your `blackduck-config.env` file, add the following:

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

Updated PostgreSQL support schedule

Starting with the upcoming **2022.10.0** release, Black Duck will end support for external PostgreSQL 11. Please see the table below for the projected dates for the beginning and end of support for future PostgreSQL versions.

PG Version	First Release	Last Release	BD External Support Added	BD External Support End
16.x	Late 2023	Late 2028	2024.7.0	2026.10.0
15.x	Late 2022	Late 2027	2023.7.0	2025.10.0
14.x	September 2021	November 2026	2022.7.0	2024.10.0

13.x	September 2020	November 2025	2021.8.0	2023.10.0
12.x	October 2019	November 2024	X	X
11.x	October 2018	November 2023	2020.6.0	2022.10.0

Japanese language

The 2022.4.0 version of the UI, online help, and release notes has been localized to Japanese.

Simplified Chinese language

The 2022.4.0 version of the UI, online help, and release notes has been localized to Simplified Chinese.

New and Changed Features in Version 2022.7.0

PostgreSQL 14 support for external databases

Black Duck now supports and recommends PostgreSQL 14 for new installations that use external PostgreSQL. Migrating to Black Duck 2022.7.x does not require migration to PostgreSQL 14.

No action is required for users of the internal PostgreSQL container.

Note: Due to an index corruption bug in PostgreSQL 14.0 through 14.3, the minimum supported version of PostgreSQL 14 is 14.4.

Split of super user role into Admin domain roles

Currently, any Black Duck user with the Super User role can create/amend the permissions of all users such that they can assign the system administrator role to any user including their own user. This leads to any Super User having the ability to gain complete access and control of the Black Duck instance, including the SysAdmin role. This appears as a privilege escalation defect however the role is functioning as intended.

In order to prevent this scenario, the Super User role has been removed and new roles have been created to handle various responsibilities formerly associated to it: Global Project Administrator, Global Project Group Administrator, User Administrator and Custom Field Administrator. Additional information on these new roles can be found in the Black Duck Help.

New Infrastructure as Code (IaC) issues display

Applications are not just the application code, the infrastructure and deployment methods are a critical component for ensuring application security. IaC is therefore being used to automate this deployment and setup of applications in different cloud and on-prem environments. These configuration options play a key role in ensuring application security and are particularly important for containerised or service based applications.

Now with Black Duck 2022.7.0, you can now see IaC issues when viewing the BOM of a project's version page if the scan included IaC. The information displayed will provide you with information needed to take action on any potential issues found in your code.

Please note that to run IaC scans, you must meet the following operating system requirements and have Detect 7.14 or later.

For more information regarding Infrastructure as Code scanning, please refer to our Community page.

Improved robustness for scan CLI

Scan CLI has been improved to prevent hanging when it completes on the server by introducing a retry mechanism. This means that scans will complete and upload normally even after Hub, scan, or nginx services restart.

New support for bulk comments for a project version components

This new feature provides the ability to add bulk comments to ease user review and curation of the BOM. For example, instead of applying comments to components individually, you can select any number of components on the project version page and add a comment to the selected items simultaneously.

New automated API access token purging

This new feature will allow User Administrators of the Black Duck system to better maintain and control access to Black Duck via access tokens by setting up a schedule to automatically purge inactive access tokens. This functionality can be found on the new **Admin** > **Access Tokens** page. You can also manually curate all existing access tokens as well through this page.

Increased binary scan container memory allocation

In order to prevent binary scans failures, we have increased the binary scan container memory from 2GB to 4GB.

Enhanced Policy Rule user experience

When creating or editing a policy, the Component Conditions will now display instructions to clarify how to add or exclude a component version to a policy when the "in" or "not in" operators are used.

Updated Black Duck KnowledgeBase search

The **Find** > **Black Duck KnowledgeBase** page has had some minor changes to its appearance and how the results are displayed after performing a search.

In the earlier releases, Black Duck KnowledgeBase searches displayed Black Duck projects and Custom Components along with KnowledgeBase components in the result set. Starting with 2022.7.0, Black Duck KnowledgeBase searches return only KnowledgeBase Component data. In order to search for Custom Components, users should leverage the Components search tab. To search for Black Duck projects, users should use the Projects search tab.

In addition, the Component Source filters on the Black Duck KnowledgeBase page (Custom Components and Black Duck Projects) have been removed.

Enhanced KnowledgeBase update job tasks

Previously, tasks that made up a KnowledgeBase update job (component, component version, license, NVD vulnerability, and BDSA vulnerability) were run in preset order. If the component task failed, subsequent tasks would not be executed. New to 2022.7.0, a continuation mechanism has been introduced that manages failed tasks, which prevents the blocking of the execution of subsequent tasks.

Additionally, this provides better optics from a jobs page perspective as long as some detail is present on why a specific task failed.

New Rapid Scan properties added

The following properties have been added to the output of Rapid Scans:

- `cweIds`: List of Common Weakness Enumeration (CWE) IDs for this security vulnerability.

- `shortTermUpgradeGuidance`: Suggested component version to upgrade to as a short term course of action to address this vulnerability as it is the same major version as the one in use.
- `longTermUpgradeGuidance`: Suggested component version to upgrade to as a long term course of action. Taking this course of action might require major version number upgrade and must be more carefully planned.

New upgrade guidance information to Detect endpoint

The following have been added to the Detect component scan results:

- `shortTermUpgradeGuidance`: Suggested component version to upgrade to as a short term course of action to address this vulnerability as it is the same major version as the one in use.
- `longTermUpgradeGuidance`: Suggested component version to upgrade to as a long term course of action. Taking this course of action might require major version number upgrade and must be more carefully planned.

Updated data retention management for project versions

You can now better manage your project versions' data retention policy. If Automatic Data Removal has been enabled in your environment, you can now select specific project versions to protect from deletion. This can be enabled when creating a new project or by editing existing project versions. When viewing your project, project versions protected from Automatic Data Removal will have a lock icon displayed at the end of its row.

Updated Software Bill of Materials (SBOM) Report type and export formats

You can now export the Software Bill of Materials report for your projects in CycloneDX v1.4 format. The CycloneDX v1.4 format includes security vulnerability information; BDSA records will now be included along with NVD records.

For more information on CycloneDX v1.4, please visit the CycloneDX v1.4 reference page.

The report type (SPDX, CycloneDX v1.3, or CycloneDX v1.4) will also be included in the report name to better identify the type used after report generation.

In addition, new report formats are available when generating a SBOM report. You can now select from JSON, YAML, RDF, and tag:value as an output for your report.

New database partition job

The Journal table is now partitioned by months. The first partition is special and contains all existing journal events. The JournalPartitionMaintenanceJob job creates new database partitions for the project audit trails and drops old partitions and Journal events older than 5 years.

Scan state/status refactoring

Previously, scan status was a design combination of scan state and scan progress which does not work well in the current queue-based scan architecture. The new approach will provide a state and then a way to track the progress of the scan as it progresses through the system. This approach should be flexible enough so the traditional scan architecture can be retrofitted so a single approach is used. State should remain in the database, while progress, being transient and updated more frequently should be moved to cache.

Reporting database enhancements

Added `exposed_on` field in `reporting.component_vulnerability` materialized view.

Minor Reporting schema change

In 2023.1.0, the type of the `basedir` column in `reporting.scan_view` will change from `character varying` to `text` to accommodate paths longer than 255 characters.

Supported browser versions

- Safari Version 15.5 (17613.2.7.1.8)
  - Safari versions 13.0 and below are no longer supported
- Chrome Version 103.0.5060.114 (Official Build) (x86_64)
  - Chrome versions 71 and below are no longer supported
- Firefox Version 102.0 (64-bit)
  - Firefox versions 71 and below are no longer supported
- Microsoft Edge Version 103.0.1264.44 (Official build) (64-bit)
  - Microsoft Edge versions 78 and below are no longer supported

Container versions

- 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
- blackducksoftware/bdba-worker:2022.6.0
- blackducksoftware/rabbitmq:1.2.10

API Enhancements

For more details on new or changed API requests, please refer to the API doc available in Black Duck.

New API to download Sigma Scanner

A new endpoint has been created to download the Sigma binary from upload-cache directly. The API request has a path variable, `arch`, which is required to indicate the desired architecture as well as an optional header parameter called `version`.

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

Fixed Issues in 2022.7.0

The following customer-reported issues were fixed in this release:

- (HUB-33231). Fixed an issue where sorting scans by scan size on the Scans page was not displaying the list in the correct order.
- (HUB-33974). Fixed an issue where the affected project count for vulnerabilities might be misleading. Ignoring a component will change the number of components with a given risk on the summary page. Vulnerability searches will not count ignored components, but the component search will.
- (HUB-32773). Fixed an issue when a component has been modified locally would cause our system to consider it a local component and not originating from the KnowledgeBase. The BOM computation would not query the KnowledgeBase when fetching new information for the component.
- (HUB-34468). Fixed issue where rapid scans would time out while waiting in queue for other, longer running scan types to finish matching.
- (HUB-34459). Fixed an issue where the `--matchConfidenceThreshold` parameter was not functioning when used with the traditional scan.cli.
- (HUB-33477). Fixed an issue where the Black Duck Metadata URL download button was available if SAML was disabled.
- (HUB-33549). Fixed an issue where the "Match Type" selection list for "**Policy Management** > **Create Policy Rule** > **Component Conditions**" doesn't have "Direct Dependency Binary" and "Transitive Dependency Binary" options.
- (HUB-34215). Updated the jackson-databind and gson components in responses to finding 4 high vulnerabilities.
- (HUB-33551). Fixed an issue where uploading a BDIO file with a null code location would fail with status code 400.
- (HUB-32919). Fixed an issue when attempting to download a scan using aggregate mode BDIO from Hub would produce a corrupt/empty BDIO of 0 bytes.
- (HUB-29445). Fixed an issue where the Projects REST API filtering did not support project names with commas.
- (HUB-33164). Fixed an issue where system logs were not downloadable from the Blackduck UI when excessive in size.
- (HUB-34282). Fixed an issue with the system_check.sh script where it could produce false warnings if the limits and reservations for memory are set to exceeding 512MB higher than Java heap size. the script has been updated to flag when the overhead is >20% and >1024Mb of memory so that smaller containers will not cause false warnings when set up in accordance to the documentation.
- (HUB-33923). Fixed an issue when refreshing the **Admin** > **Diagnostics** > **System Information** > **Job page**, the statistics for job history could display significantly different counts.
- (HUB-34195). Updated the REST API documentation to remove `SBOM` as a value from `reportType` from the Creating a Version Report section (or the `/api/versions/{projectVersionId}/reports` request).

- (HUB-34296). Fixed an issue where the policy override date info cannot be displayed in Japanese settings due to an incorrect i18n character.
- (HUB-32008). Fixed an issue where the Security Risk Ranking page can get stuck Processing due to "Up-to-date with error" events not being auto-cleaned-up by the QuartzVersionBomEventCleanupJob job.
- (HUB-33727). Fixed a UI bug when updating remediation status or comment of a vulnerability (In Security tab of Project Version).
- (HUB-33691). Fixed a UI bug where the warning icons were missing on the Cryptography tab for encryption algorithms with known weaknesses.
- (HUB-34240). Fixed an issue with the `/api/projects/{projectId}/custom-fields/{customFieldId}` request where it could generate a 400 error when posting a null value.
- (HUB-34246). Fixed browser display issues on the Project Version Comparison view.
- (HUB-33246). Clarified the REST API documentation; replaced references to `https://.../` for `https://<server-url>/api/`.
- (HUB-33481). Fixed an issue with the inconsistent response of `/api/projects/{pid}/versions/{vid}/matched-files?offset={larger than totalCount}` between 2021.8.x and later versions. The matched-files endpoint should return now consistently return a 200 OK response with empty items even if the offset > totalCount.
- (HUB-34468). Fixed an issue where Rapid Scan was failing with the following error: "Error getting developer scan result. Timeout may have occurred." or a HTTP 404 Not Found response caused by a delay in the match engine.
- (HUB-33512). Updated the text for Test Connection, User Authentication and Field Mapping found under **Administration** > **Settings** > **User Authentication**. Removed the mention of "and shows result of mapping test-user's meta-data".
- (HUB-34836). Fixed an issue where it was possible to edit unmatched components as the project itself when the BLACKDUCK_HUB_SHOW_UNMATCHED flag was enabled.
- (HUB-34380). Fixed an issue when trying to scan a new version into a project that has had a very large number of adjustments made to it could cause the BOM scan of the new version to fail on the server with the message "Exception occurred Too many parameters".
- (HUB-33793). Fixed an issue where Project Version details report was failing when a registration key not licensed with “Black Duck Security Advisory” was used with a change in security risk ranking.
- (HUB-33375). Fixed some bad SQL grammar in the query building code where ORDER_BY was outside of the loop that determines which field by which to sort. If there were no sort fields, the ORDER_BY would be null.
- (HUB-34780). Fixed an issue where the statistics on Administration > Diagnostics > usage: project > Project_created/Version_Created/Version_Deleted was limited to 500 even if more than 500 projects/version were created or deleted.
- (HUB-34592). Fixed a deserialization of CodeLocationBomMatchCacheEntry error when there are zero matched components, but both empty and existing fails in the test.
- (HUB-34588). Fixed an issue with the copyright links for the conan package not working due to unencoded hash character in link.
- (HUB-24664). Fixed an issue where BDSBackgroundUpdateWorker was still trying to communicate out to the registration servers over HTTP rather than HTTPS.
- (HUB-33679). Fixed an issue where MaaS enabled scans sometimes fail when extracting composite elements.

- (HUB-34218). Updated the REST API documentation to include "componentVersionName" and "componentVersion" for "BOM Component Representation".

Black Duck SCA 2022.4.x

New and Changed Features in Version 2022.4.2

Improved performance on database migration script

Performance improvements have been made to the database migration script used when upgrading Black Duck versions resulting in faster installation times.

Container versions

- 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
- blackducksoftware/bdba-worker:2022.3.0
- blackducksoftware/rabbitmq:1.2.7

API Enhancements

For more details on new or changed API requests, please refer to the API doc available in Black Duck.

Fixed Issues in 2022.4.2

Black Duck 2022.4.2 contains no fixed customer-reported issues.

New and Changed Features in Version 2022.4.1

New BDSA Auto Remediation setting to automatically ignore CVEs with related unmatched BDSA records

Activating this setting will automatically remediate new CVE vulnerabilities with related unmapped BDSAs by setting the remediation status to IGNORED and adding a message to describe why the vulnerability was remediated.

This new setting only applies to CVE vulnerabilities with a related BDSA vulnerability. If the CVE is mapped to a component version, but its related BDSA is not also mapped to that component version then the system may automatically remediate the CVE vulnerability based on the system setting.

The BDSA Auto Remediation feature can be enabled from the Admin > System Settings > BDSA Auto Remediation page.

New Rapid Scan properties added

The following properties have been added to the output of Rapid Scans:

- `cweIds`: List of Common Weakness Enumeration (CWE) IDs for this security vulnerability.
- `shortTermUpgradeGuidance`: Suggested component version to upgrade to as a short term course of action to address this vulnerability as it is the same major version as the one in use.
- `longTermUpgradeGuidance`: Suggested component version to upgrade to as a long term course of action. Taking this course of action might require major version number upgrade and must be more carefully planned.

Improved user permission evaluations performance

Improvements were made to user permission evaluations for most API requests. This should result in more consistent loading times including loading BOMs regardless of the user's role or permissions.

Updated Black Duckctl

Black Duckctl has been updated to 3.0.1 to add Black Duck 2022.4.0 installation support for sizes-gen03 deployment sizes.

Container versions

- 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
- blackducksoftware/bdba-worker:2022.3.0
- blackducksoftware/rabbitmq:1.2.7

API Enhancements

For more details on new or changed API requests, please refer to the API doc available in Black Duck.

Performance Improvements for project endpoints

The following API project endpoints were found to be underperforming and have been optimized:

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

Fixed Issues in 2022.4.1

The following customer-reported issues were fixed in this release:

- (HUB-32395, HUB-33033). Fixed an issue where the modified declared license to matched component is sometimes not displayed on SPDX reports.
- (HUB-29532). Fixed an issue where Linux distro package matching was broken when the rootfs pathin an distro image was not starting at the root directory but at a subdirectory.
- (HUB-33947). Fixed an issue where the Security Risk was not updated when updating the Remediation Status from 'Affected Projects' page.
- (HUB-33551). Fixed an issue when uploading a bdio file with code location name as null, the request would fail with the status code 400 and throwing exception in background.
- (HUB-34065). Fixed SPDX 2.2 report format that was causing the following error in the SPDX validation tools:

  ```
  The following warning(s) were raised: [object instance has properties which are not
   allowed by the schema: ["packageSupplier"] for {"pointer":"/packages/0"}
  ```
- (HUB-33616). Fixed an issue where the scan client would in some cases (when there are duplicated archive entries inside scanned archive), generate a BDIO with incorrect ids, which in turn could produce an error when the bdio file is stored to the database.
- (HUB-33915, HUB-33865). Fixed an issue where the scan upload API submitted the entire scan data as one message into RabbitMQ without chunking, causing a message size error.
- (HUB-24664). Fixed an issue where the registration container logs were showing attempted communication over HTTP.
- (HUB-33579). Fixed an issue where the `--matchConfidenceThreshold` parameter was not functioning when used with the traditional scan.cli.
- (HUB-33311). Fixed an issue where the signature scanner could fail with the error code 74. A retry function was introduced to mitigate this error.

Announcements for Version 2022.4.0

Security Advisory for Spring Framework (CVE-2022-22965)

Black Duck is aware of the disclosed security issue relating to the Spring Framework open source software, CVE-2022-22965 (tracked in the Black Duck KnowledgeBase™ as BDSA-2022-0858), disclosed on March 30th, 2022. For more information about the vulnerability, see the official CVE entry: https://tanzu.vmware.com/security/cve-2022-22965

On March 31st, 2022, Spring released Spring Framework versions 5.3.18 & 5.2.20, which address the vulnerability described by CVE-2022-22965.

Currently, Black Duck believes there is limited exposure to Black Duck SIG products, services, and systems. To the extent we have had exposure, we have applied mitigations that prevent attempted exploitation. We have completed all internal investigations and the results of those investigations can be found in the "Product Status" section of our Community advisory page.

Finally, to be clear, the previously mentioned investigation is focused exclusively on CVE-2022-22965 (Spring Framework) and should not be confused with CVE-2022-22963 (Spring Cloud Function).

At the time of publication, Black Duck has not identified any exposure to CVE-2022-22963 (tracked in the Black Duck Hub KnowledgeBase™ as BDSA-2022-0850) in SIG products. If new details become available which change this evaluation, a separate advisory for CVE-2022-22963 will be published.

Upgrading to Black Duck 2022.4.0

Please note that upgrading to Black Duck 2022.4.0 may take longer than expected due to the execution of migration scripts and other new processes introduced in this version. More details can be found in the New and Changed Features section below.

Resource Guidance Changes

The default resource settings have updated and the recommended settings have increased for all scan volumes. The previous resource settings are still available and have been moved to new directories as described below, but their use is discouraged.

Please note, the exact possible scan throughput will vary based on your scan size, type and composition. However, we used this breakdown in our internal testing to gather the information in the table below:

- 50% full signature scans
- 40% full package manager scans
- 10% developer package manager scans

Container resource limits

Starting with Black Duck 2022.4.0, all containers will have resource limits set, whereas previously, some containers did not. For example, previous resource allocations did not set a CPU limit for the bomengine container, so it could use CPU disproportionate to the containers with limits. Since the new sizes below do not allow unbounded CPU usage, customers may see a decrease in scan throughput if they choose one of the new sizes that looks close to the old limits.

File organization changes

In addition to the changes mentioned above, the organization of resource override YAML files has changed.

For Kubernetes, the organization of resource override YAML files in the Helm chart has changed:

- The `values` folder has been renamed to `sizes-gen01`.

- The 4 previous t-shirt size files (`small.yaml`, etc.) have been moved to the new `sizes-gen02` directory.
- A new directory, `sizes-gen03`, now contains a resource overrides file for each of the configurations named in the table below; they are named `10sph.yaml`, `120sph.yaml`, etc.

For Swarm, Black Duck no longer allocates container resources directly in `docker-compose.yml`. Instead, resources are specified in a separate overrides file. The previous resource allocations, from Black Duck versions 2022.2.0 and earlier, have been moved to `sizes-gen02/resources.yaml`. Starting with Black Duck 2022.4.0 and later, multiple possible allocations will be provided in the `sizes-gen03 folder`.

For both Kubernetes and Swarm, there are 7 allocations based on load as measured in average scans per hour; if your anticipated load does not match one of the predefined allocations, round up. For example, if you anticipate 100 scans per hour, select `sizes-gen03/120sph.yaml`.

Resource Guidance & Container Scalability

These settings apply to both Kubernetes and Swarm installations.

Name	Scans/Hour	Black Duck Services	PostgreSQL	Total
10sph	10	CPU: 12 core Memory: 30 GB	CPU: 2 core Memory: 8 GB	CPU: 14 core Memory: 38 GB
120sph	120	CPU: 13 core Memory: 46 GB	CPU: 4 core Memory: 16 GB	CPU: 17 core Memory: 62 GB
250sph	250	CPU: 17 core Memory: 118 GB	CPU: 6 core Memory: 24 GB	CPU: 23 core Memory: 142 GB
500sph	500	CPU: 28 core Memory: 210 GB	CPU: 10 core Memory: 40 GB	CPU: 38 core Memory: 250 GB
1000sph	1000	CPU: 47 core Memory: 411 GB	CPU: 18 core Memory: 72 GB	CPU: 65 core Memory: 483 GB
1500sph	1500	CPU: 66 core Memory: 597 GB	CPU: 26 core Memory: 104 GB	CPU: 92 core Memory: 701 GB
2000sph	2000	CPU: 66 core Memory: 597 GB	CPU: 34 core Memory: 136 GB	CPU: 100 core Memory: 733 GB

PostgreSQL Settings

Customers using the PostgreSQL container will need to set the values manually using ALTER SYSTEM, and changes to `shared_buffers` won't take effect until after the next time that PostgreSQL is restarted. These settings apply to both Kubernetes and Swarm installations.

Name	Scans/Hour	PostgreSQL CPU/ Memory	shared_buffers (MB)	effective_cache_size (MB)
10sph	10	CPU: 2 core Memory: 8 GB	2654	3185
120sph	120	CPU: 4 core Memory: 16 GB	5338	6406
250sph	250	CPU: 6 core Memory: 24 GB	8018	9622

500sph	500	CPU: 10 core Memory: 40 GB	13377	16053
1000sph	1000	CPU: 18 core Memory: 72 GB	24129	28955
1500sph	1500	CPU: 26 core Memory: 104 GB	34880	41857
2000sph	2000	CPU: 34 core Memory: 136 GB	45600	54720

Upcoming PostgreSQL 9.6 deprecation

As previously announced, support for running Black Duck on PostgreSQL 9.6 ended with the 2021.6.0 release of Black Duck. Starting with the 2022.7.0 release of Black Duck, attempting to run Black Duck with PostgreSQL 9.6 will generate an error, and Black Duck will fail to start.

End of support for Desktop Scanner on RHEL 7 and CentOS 7

As of 2022.4.0, Black Duck will no longer build new versions of the Desktop Scanner for Red Hat Enterprise Linux 7 and CentOS 7. Additionally in the upcoming 2022.7.0 release, the binaries will be dropped altogether.

Updated PostgreSQL support schedule

Starting with the upcoming **2022.10.0** release, Black Duck will end support for external PostgreSQL 11. Please see the table below for the projected dates for the beginning and end of support for future PostgreSQL versions.

PG Version	First Release	Last Release	BD External Support Added	BD External Support End
16.x	Late 2023	Late 2028	2024.7.0	2026.10.0
15.x	Late 2022	Late 2027	2023.7.0	2025.10.0
14.x	September 2021	November 2026	2022.7.0	2024.10.0
13.x	September 2020	November 2025	2021.8.0	2023.10.0
12.x	October 2019	November 2024	X	X
11.x	October 2018	November 2023	2020.6.0	2022.10.0

Azure PostgreSQL 13 Flex Server Configuration

When installing Black Duck, Azure users may encounter the following error message when running the `external-postgres-init.pgsql` init script:

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

To prevent this error, ensure that server parameter '`azure.extensions`' has value '`PGCRYPTO`' when using Azure PG 13 Flex Server.

Deprecrated APIs

The following legacy API Solr endpoints have been deprecated and will be removed in the Black Duck 2022.7.0 release:

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

Japanese language

The 2022.2.0 version of the UI, online help, and release notes has been localized to Japanese.

Simplified Chinese language

The 2022.2.0 version of the UI, online help, and release notes has been localized to Simplified Chinese.

New and Changed Features in Version 2022.4.0

Spring Framework Update

Spring Framework has been updated to 5.3.18 to address the critical CVE-2022-22965 vulnerability.

New vulnerability metrics comparison

This new feature makes a change to a vulnerability's Overview page so that you can now see a side-by-side view of the metrics where applicable. When viewing a vulnerability that has both a BDSA and NVD record, you will see a graph in the Scores and Metrics section comparing both vulnerability types; BDSA and NVD. You can also alternate between CVSS v2 and CVSS v3.x to get more information.

Git repository SCM Integration - Phase 1

Black Duck 2022.4.0 is introducing a way to simplify onboarding of new projects for customers by leveraging integrations for management of repositories, branches, builds, and releases. Starting with Phase 1, we are adding a new SCM URL field to the Create Project modal and Project Settings page, and a SCM Branch field to the Project Version Settings page.

These fields are manually populated in this phase. However, in an upcoming Detect release, they will be automatically populated after scanning a git repository. Detect will automatically identify the associated git repository URL and branch and then send that information to Black Duck.

Please note that this feature is not enabled by default in Black Duck and must be activated by adding the following in your environment:

For Swarm users, add this to your `docker-compose.yml` webapp environment:

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

For Kubernetes users, add this to your webapp container environment:

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

New Components tab for BDSA vulnerabilities

A new Components tab has been added to BDSA vulnerability records. This tab will allow you to see all known component versions affected by a particular BDSA vulnerability.

Enhanced Component dashboard materialized view query

All the queries relating to the SearchDashboardRefreshJob have been optimized for better performance. The LicenseDashboardRefreshJob is longer available and the view relating to it will be refreshed under SearchDashboardRefreshJob. This means the counts displayed in the License Management page will now be updated as SearchDashboardRefreshJob finishes.

NOTE: As a result of these changes, upgrading to Black Duck 2022.4.0 may take longer than usual due to the execution of migration scripts.

PostgreSQL 11 container migration

In Kubernetes and OpenShift deployments using the Black Duck-provided PostgreSQL container, the following persistent volume claim added in 2022.2.0 is no longer needed. It and its associated persistent volume may be safely deleted.

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

Updated Java heap size allocation and new environment variable

In previous releases, Java was allowed to slowly increase its heap size up to `HUB_MAX_MEMORY`. Starting with Black Duck 2022.4.0, in order to take advantage of efficiencies and predictability, we will now pre-allocate the entire `HUB_MAX_MEMORY` on startup.

As part of this update, a new environment variable has been added: `HUB_MIN_MEMORY`. This variable will allow you to set the lower boundary for Java heap size.

By default and as the optimal setting, `HUB_MIN_MEMORY` is set equal to `HUB_MAX_MEMORY`, but can be set explicitly to a smaller amount (for example, 512m) to allow Java, once again, to acquire memory gradually starting from `HUB_MIN_MEMORY` to no more than `HUB_MAX_MEMORY`.

Limit Rapid Scan policy overrides to specific vulnerabilities

In previous Black Duck versions, Rapid Scan policy violations could be overridden by policy and component. However, if new vulnerabilities were subsequently found, existing overrides could suppress the violation, resulting in a false negative.

Now in Black Duck 2022.4.0, you can now override a specific vulnerability in rapid scans using the existing yaml upload mechanism.

The vulnerability Id is validated to match the expected format.

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

New Rapid Scan vulnerability properties added

The following properties have been added to vulnerabilities in the output of Rapid Scans:

- publishedDate (Date value)
- vendorFixDate (Date value)
- workaround (String value)
- solution (String value)

New BDSA Automatic Remediation setting (Beta)

When the Black Duck Security Advisory (BDSA) team analyzes a CVE vulnerability, they check to see what component versions are affected by the vulnerability. Sometimes they find that the vulnerability applies to a different set of versions. This new feature will give you the ability to automatically ignore CVE vulnerabilities if the BDSA team has found that the vulnerability does not apply to that component version. This only affects vulnerabilities with the NEW status.

The BDSA Automatic Remediation is a **beta feature** and is **not** enabled by default. To enable this feature, the following environment variable must be set:

```
BDSA_AUTO_REMEDIATION=true
```

The BDSA Auto Remediation setting can then be changed on the **Admin** > **System Settings** > **BDSA Auto Remediation** page.

Note: Whenever the user saves the setting, the system checks and may update vulnerabilities for all projects. On large systems, this can take a long time and have an impact on Black Duck performance.

Updated Users & Groups management display

The look and feel of the Users and Groups tabs under Admin > Users & Groups have been updated to display more cleanly by breaking up the various sections (User/Group Details, Overall Roles, Project Groups, Projects, Users/User Groups) into their own individual pages making it easier to manage your users and groups.

New Component Condition rule for policies

A new component condition for Unconfirmed Snippets has been added. The new policy condition gives you the ability to create or edit a policy that allows you to trigger a policy violation for snippets that have not been reviewed.

New Software Bill of Materials (SBOM) Report CycloneDX v1.3 export format

You can now export the Software Bill of Materials report for your projects in CycloneDX v1.3 format. This can be done by viewing a project version, clicking the Reports tab, clicking the Create Report button, and then selecting CycloneDX v1.3 - JSON. For more information on CycloneDX v1.3, please visit the CycloneDX v1.3 reference page.

New Component Dependency Duplication Sensitivity system property

A new system property has been added to Black Duck to control the maximum number of nodes (matches) per component added to resulting dependency tree in package manager scan:

```
blackduck.match.limit.per.component
```

The default value of this system property is 10, thus the number of duplicated components in the tree can not exceed the `blackduck.match.limit.per.component` value (match limit per component).

Supported browser versions

- Safari Version 15.4 (16613.1.17.1.13, 16613)
  - Safari versions 13.0 and below are no longer supported
- Chrome Version 100.0.4896.75 (Official Build) (x86_64)
  - Chrome versions 71 and below are no longer supported
- Firefox Version 99.0 (64-bit)
  - Firefox versions 71 and below are no longer supported
- Microsoft Edge Version 100.0.1185.36 (Official build) (64-bit)
  - Microsoft Edge versions 78 and below are no longer supported

Container versions

- 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
- blackducksoftware/bdba-worker:2021.12.2
- blackducksoftware/rabbitmq:1.2.7

API Enhancements

For more details on new or changed API requests, please refer to the API doc available in Black Duck.

Performance Improvements for project endpoints

The following API project endpoints were found to be underperforming and have been optimized:

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

Fixed Issues in 2022.4.0

The following customer-reported issues were fixed in this release:

- (HUB-33047). Fixed an issue where Null Pointer Exception errors occurring during the KbUpdateJob process could cause the job to progress very slowly or appear to be stuck.
- (HUB-32336). Renamed the Components filter on the BOM page to Component Versions to bring it in line with the actual functionality.
- (HUB-32316). Fixed an issue where the HUB_MAX_MEMORY environment variable to define maximum memory allocation pool for the JVM was left unset in docker registration container deployments.
- (HUB-32492). Fixed an issue where components with the MIT license could trigger a policy violation for "License Not Approved" and "License Unreviewed" in Rapid Scan, although MIT License is set as "Approved" in BlackDuck.
- (HUB-31839). Fixed an issue where the BDIO upload endpoint project and version values were not URL decoded.
- (HUB-32692, HUB-32672). Fixed an issue where if a component had multiple vulnerabilities, each with different vulnerability statuses, policy rules would not trigger a policy violation unless all the vulnerabilities for the component matched the selected policy rules.
- (HUB-31872). Fixed an issue where Rapid Scans did not validate the user permissions. If a scan finds a matching project version BOM but the user does not have permission - the scan will run without project version or BOM component data.
- (HUB-33231). Fixed an issue where sorting scans by scan size on the Scans page was not displaying the list in the correct order.
- (HUB-33096). Fixed an issue where filtering by license family may not display modified KnowledgeBase licenses correctly.
- (HUB-30463). Fixed an issue where the golang.org/x/sys component was not displaying in the Hub UI KnowledgeBase search.
- (HUB-31891). Fixed an issue where searching for the "Apache HTTP Server" component would link to the debian component page.
- (HUB-28406). Fixed an issue where sometimes a different number of vulnerabilities would be shown on the Security Tab and the Details Tab in some OSS component and versions.
- (HUB-32883). Fixed an issue where the accessTokenValiditySeconds setting's Max-Age and Expires fields did not align with the expiry value of the JSON Web Token (JWT).
- (HUB-32313). Fixed a performance issue with the REST API `/api/projects/<id>/versions/<id>/components` endpoint when dealing with a high package manager scan data load.
- (HUB-32571). Fixed an issue with how the namespace of origin was displayed inconsistently in the component version Copyrights tab and Black Duck notice reports (and BOM Security tab).
- (HUB-32949). Fixed an issue where having a user directly assigned to a Project Group and the same user assigned to a User Group that's also assigned to the Project Group would result in multiple project groups being returned by the API, resulting in a Detect failure.
- (HUB-33132). Fixed an issue where the dependency-paths API was consuming large amount of service memory and paging to disk.
- (HUB-33155). Fixed an issue where refreshes of HUB registration could stall, causing the jobrunner to hold a lock much longer than it should potentially resulting in blocked queries.

- (HUB-32010). Fixed an issue where when navigating through the Project Groups hierarchy, clicking a project within a subgroup could return the user back to the root project group.
- (HUB-32977). Fixed an issue where mixed case tags were not triggering policy rules as expected.
- (HUB-33305). Fixed an indentation issue in the `docker-compose.local-overrides.yml` file.
- (HUB-27940). Fixed an issue when deploying to EKS, without a minimum CPU resource specified, the pod will be allocated .25 (250m) CPU core causing bomengine/rabbitmq to not work.
- (HUB-33455). Fixed an issue where the link to the Vulnerability Detail Page for CVE-2022-23395 would go to a 404 Not Found error page.
- (HUB-32256). Fixed an issue where submitting an empty value for the custom signature level would generate an incorrect error message.
- (HUB-32800). Fixed an issue where the matchengine could restart or jobs could hang in jobrunner during bitbake/yocto scans due to very large numbers of matches per component in dependency tree resulting in OutOfMemory exceptions. See the New Component Dependency Duplication Sensitivity system property item in the New and Changed Features section above for more details.
- (HUB-33349). Fixed an issue where the webapp container needed a persistent volume named "`{{ .Release.Name }}-blackduck-webapp`" by default where "`Release.Name`" is typically "`hub`" or another label chosen at deployment time. In addition, some customers may have configured a custom persistent volume name by configuring the `persistentVolumeClaimName` in the webapp `values.yaml` overrides. These configurations, the persistent volume and the persistent volume claim, are no longer necessary and can be safely deleted.
- (HUB-32678). Fixed an issue where the default IP scan was not supporting the scan.cli argument `--matchConfidenceThreshold` to filter matched components.
- (HUB-29532). Fixed an issue where Linux distro package matching was broken when the rootfs path in an distro image was not starting at the root directory but at a subdirectory.

Black Duck SCA 2022.2.x

New and Changed Features in Version 2022.2.2

Black Duck version 2022.2.2 is a maintenance release and contains no new or changed features. A fix was made to the online help to prevent a security vulnerability.

Container versions

- 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
- blackducksoftware/bdba-worker:2021.12.2
- blackducksoftware/rabbitmq:1.2.7

API Enhancements

For more details on new or changed API requests, please refer to the API doc available in Black Duck.

Fixed Issues in 2022.2.2

The following customer-reported issues were fixed in this release:

- (HUB-34065). Fixed SPDX 2.2 report format that was causing the following error in the SPDX validation tools:

```
The following warning(s) were raised: [object instance has properties which are not
 allowed by the schema: ["packageSupplier"] for {"pointer":"/packages/0"}
```

New and Changed Features in Version 2022.2.1

Updated Data Removal feature (Beta)

The data removal feature allows you to explore ways to automatically delete ProjectVersions according defined criteria. For users with version limits, disk space constraints or database bottlenecks, the buildup of obsolete versions can become problematic to either their process or to their system performance. This feature is helpful if you generate multiple ProjectVersions over time which become obsolete over time.

Added in Black Duck 2022.2.0, a new environment variable has been added:

- `BLACKDUCK_AUTOMATIC_VERSION_REMOVAL_RELEASE_PHASES`
  - Defines what ProjectVersion phases are applicable to the data removal process.
  - Release phases values are: Planning, Development, Released, Deprecated, Archived, and Prerelease
  - If not set, the default value is Development.
  - Values are case insensitive.
  - Multiple release phases can be added with the phases delimited by comma.

Updated role assignment for Projects and Project Groups

You can now add users to Projects and Project Groups as a Project Viewer. When adding a user to a Project or Project Group, the role of Project Viewer is now automatically selected and serves as the default role. You can then add further roles to the user as needed.

Updated minimum scan interval configuration

Starting from Detect 7.13 and later, the Black Duck Hub scan setting for Minimum Scan Interval will be disabled. Minimum scan interval should be configured as a command argument through Detect as follows:

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

where ## is the time in hours.

Container versions

- 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
- blackducksoftware/bdba-worker:2021.12.2
- blackducksoftware/rabbitmq:1.2.7

API Enhancements

For more details on new or changed API requests, please refer to the API doc available in Black Duck.

Fixed Issues in 2022.2.1

The following customer-reported issues were fixed in this release:

- (HUB-32540). Fixed a rare issue with the KbUpdateJob where a duplicate value insert could slow down or fail the job.
- (HUB-32544). Fixed a race condition issue where the KbUpdateJob tries to insert a `version_bom_component` already inserted by a scan.
- (HUB-33045). Fixed an issue where creating a policy rule specifically for Rapid Scans could cause all project versions to enter a re-computation state where the BOM's Status would change to "Processing".
- (HUB-32363 and HUB-33027). Fixed a possible race condition while unmapping code location for the following scenarios (without using --detect.project.codelocation.unmap=true):
  - Code location is rescanned and mapped to other project version.

  - Code location is manually unmapped from UI.
  - Code location is manually deleted from UI.
  - Code location is deleted by ScanPurgeJob.
- (HUB-33155). Fixed an issue where refreshes of HUB registration could stall, causing the jobrunner to hold a lock much longer than it should potentially resulting in blocked queries.
- (HUB-33132). Fixed an issue where the dependency-paths API was consuming large amount of service memory and paging to disk.
- (HUB-31212). Fixed an issue where members of one sub-project group could access all project groups and their tree.
- (HUB-33162). Fixed an issue where vulnerability results in Rapid Scans could display incorrect information when the highest priority Security Risk Ranking set does not match the vulnerability type (BDSA vs NVD) and the CVSS preference.
- (HUB-31756). Fixed an issue where the Project Viewer and Project Group Viewer roles were not assignable to users added to Projects and Project Groups.
- (HUB-33047). Fixed an issue where Null Pointer Exception errors occurring during the KbUpdateJob process could cause the job to progress very slowly or appear to be stuck.

Announcements for Version 2022.2.0

Enhanced Signature Generation

Starting with Black Duck 2022.2.0, the Signature Scanner will default to generation of signatures on the client rather than the server.

If you are using the Blackduck hosted service or if you are using the Helm Charts or Docker Swarm 'yaml' files included in the release, this change will be seamless with no action is required on your part. There will not be any interruption to your service.

However, if you have customized your Helm Charts or use an override file, please refer to Rebalancing Guidance on our Community page for additional information to assist you with the transition.

Page Limit Maximums on API Requests

In an ongoing effort to better manage system resources, a maximum page limit has been introduced to certain API requests. The maximum page limit will be set to 1000 pages with the possibility of change in future Blackduck versions. See the API Enhancements section below for a list of the affected API requests in the 2022.2.0 version.

Deprecated APIs

With Blackduck 2022.2.0, the `/cpes/{cpeId}/variants` endpoint will be deprecated, to be replaced with `/cpes/{cpeId}/origins`. The `/cpes/{cpeId}/variants` will be removed in Blackduck 2022.4.0. The API link in the metadata for `/api/cpes` has also been updated to return `/api/cpes/{cpeId}/origins` instead of `/api/cpes/{cpeId}/variants`.

Upcoming Resource Guidance Changes

In the upcoming Black Duck 2022.4.0 release, the default resource settings will be updated and the recommended settings will increase for all scan volumes. The 2022.4.0 release will be accompanied by instructions on how to continue to use the existing settings.

Please note, the exact possible scan throughput will vary based on your scan size, type and composition. However, we used this breakdown in our internal testing to gather the information in the table below:

- 50% full signature scans
- 40% full package manager scans
- 10% developer package manager scans

File Organization Changes

In addition to the changes mentioned above, starting in 2022.4.0, the organization of resource override YAML files will change.

For Kubernetes, the organization of resource override YAML files in the Helm chart will change.

- The `values` folder will be renamed to `sizes-gen01`.
- The 4 previous t-shirt size files (`small.yaml`, etc.) will be moved to the new `sizes-gen02` directory.
- A new directory, `sizes-gen03`, will contain a resource overrides file for each of the configurations named in the table below; they are named `10sph.yaml`, `120sph.yaml`, etc.

For Swarm, Black Duck will no longer allocate container resources directly in `docker-compose.yml`. Instead, resources will be specified in a separate overrides file. The current resource allocations will be moved to `sizes-gen02/resources.yaml`. For Black Duck 2022.4.0 and later, multiple possible allocations will be provided in the `sizes-gen03 folder`.

For both Kubernetes and Swarm, there will be 7 allocations based on load as measured in average scans per hour; if your anticipated load does not match one of the predefined allocations, round up. For example, if you anticipate 100 scans per hour, select `sizes-gen03/120sph.yaml`.

Resource Guidance & Container Scalability

These settings will apply to both Kubernetes and Swarm installations.

Name	Scans/Hour	Black Duck Services	PostgreSQL	Total
10sph	10	CPU: 10 core Memory: 29 GB	CPU: 2 core Memory: 8 GB	CPU: 12 core Memory: 37 GB
120sph	120	CPU: 12 core Memory: 46 GB	CPU: 4 core Memory: 16 GB	CPU: 16 core Memory: 62 GB
250sph	250	CPU: 16 core Memory: 106 GB	CPU: 6 core Memory: 24 GB	CPU: 22 core Memory: 131 GB
500sph	500	CPU: 27 core Memory: 208 GB	CPU: 10 core Memory: 40 GB	CPU: 37 core Memory: 249 GB
1000sph	1000	CPU: 47 core Memory: 408 GB	CPU: 18 core Memory: 72 GB	CPU: 65 core Memory: 480 GB
1500sph	1500	CPU: 66 core Memory: 593 GB	CPU: 26 core Memory: 104 GB	CPU: 92 core Memory: 697 GB
2000sph	2000	CPU: 66 core Memory: 593 GB	CPU: 34 core Memory: 136 GB	CPU: 100 core Memory: 729 GB

PostgreSQL Settings

Customers using the PostgreSQL container will need to set the values manually using ALTER SYSTEM, and changes to `shared_buffers` won't take effect until after the next time that PostgreSQL is restarted. These settings will apply to both Kubernetes and Swarm installations.

Name	Scans/Hour	PostgreSQL CPU/ Memory	shared_buffers (MB)	effective_cache_size (MB)
10sph	10	CPU: 2 core Memory: 8 GB	2654	3185
120sph	120	CPU: 4 core Memory: 16 GB	5338	6406
250sph	250	CPU: 6 core Memory: 24 GB	8018	9622
500sph	500	CPU: 10 core Memory: 40 GB	13377	16053
1000sph	1000	CPU: 18 core Memory: 72 GB	24129	28955
1500sph	1500	CPU: 26 core Memory: 104 GB	34880	41857
2000sph	2000	CPU: 34 core Memory: 136 GB	45600	54720

Japanese language

The 2021.10.0 version of the UI, online help, and release notes has been localized to Japanese.

Simplified Chinese language

The 2021.10.0 version of the UI, online help, and release notes has been localized to Simplified Chinese.

New and Changed Features in Version 2022.2.0

Logstash Update

In order to address the CVE-2021-44832 vulnerability, the Logstash image used in Black Duck has been upgraded to 7.16.3 which uses Log4j2 version 2.17.1.

Enhanced Signature Generation

As mentioned in the Announcements, the Signature Scanner will default to generation of signatures on the client rather than the server.

If you are using the Blackduck hosted service or if you are using the Helm Charts or Docker Swarm ‘yaml’ files included in the release, this change will be seamless and no manual action is required. There will not be any interruption to your service.

However, if you have customized your Helm Charts or use an override file, please refer to our *Rebalancing Guidance* article on Community for additional information to assist you with the transition.

You can also find more information regarding Monitoring Black Duck using Prometheus and Grafana on Community.

Rapid Scan Enhancements

The same endpoints are used but a new header was added to accept the rapid scan mode. New HTTP header is named 'X-BD-RAPID-SCAN-MODE' and accepts the following values:

- ALL: The default operation. It will evaluate policy rules that are RAPID or (RAPID and FULL). When the header is null this is the default.
- BOM_COMPARE: Will evaluate all policy rules like ALL, but will now evaluate differently based on the type of policy rule modes. When the policy rule is (RAPID and FULL) it will behave like BOM_COMPARE_STRICT but if the the policy rule is only (RAPID) it will behave like ALL. Policies that are only are RAPID will have a null policy status in the results.
- BOM_COMPARE_STRICT: Will only evaluate policy rules that are (RAPID and FULL). All policy rules found in the positive result will have statuses of NEW or RESOLVED. Policy violations are compared to the existing project version BOM. If the policy violation was already known and visible in the BOM (active or overridden) it is not part of the rapid scan positive result, it will still be part of the full result following existing restrictions.

In order to run either of the BOM_COMPARE modes there must be an existing project version in HUB.

PostgreSQL 11 Container Migration

The CentOS PostgreSQL 9.6 container has now been replaced by the Blackduck PostgreSQL 11 container. The new `blackduck-postgres-upgrader` container will migrate the database from PostgresSQL 9.6 to PostgreSQL 11 and will exit upon completion.

Customers with non-core PG extensions are STRONGLY encouraged to uninstall them before migrating and reinstall them after the migration completes successfully; otherwise, the migration is likely to fail.

Customers with replication set up will need to follow the instructions in the pg_upgrade documentation BEFORE they migrate. If the preparations described there are not made, the migration will likely succeed, but the replication setup will break.

IMPORTANT: Before starting the migration:

- Ensure that you have an extra 10% disk space to avoid unexpected issues arising from disk usage due to the data copying of system catalogs.
- Review root directory space and volume mounts to avoid running out of disk space as this can cause Linux system disruptions.

Updating to 2022.2.0 with **synopsysctl** will perform the following tasks:

- Stop the Black Duck instance
- Run a database migration job for users of the Black Duck-supplied PG container
- Update and restart the instance

For Kubernetes and OpenShift users:

- The migration is performed by a one-time job:
  - Stop Black Duck; e.g.,

    ```
    kubectl scale --replicas=0 -n <your_namespace> deployments --selector
     app=blackduck
    ```

  - Run the upgrade job; e.g.,

    ```
    helm upgrade <your_deployment_name> . -n <your_namespace>
     <your_normal_helm_options> --set status=Stopped --set runPostgresMigration=true
    ```

  - Restart Black Duck as normal with `helm upgrade`.

    - This migration replaces the use of a CentOS PostgreSQL container with a Black Duck-provided container. Also, the `synopsys-init` container is replaced with the `blackduck-postgres-waiter` container.
- On plain Kubernetes, the container of the upgrade job will run as root. However, the only requirement is that the job runs as the same UID as the owner of the PostgreSQL data volume.
- On OpenShift, the upgrade job assumes that it will run with the same UID as the owner of the PostgreSQL data volume.

For Swarm users:

- The migration is completely automatic; no extra actions are needed beyond those for a standard Black Duck upgrade.
- The `blackduck-postgres-upgrader` container MUST run as root in order to make the layout and UID changes described above.
- On subsequent Black Duck restarts, blackduck-postgres-upgrader will determine that no migration is needed and immediately exit.
- OPTIONAL: After a successful migration, the blackduck-postgres-upgrader container no longer needs to run as root.

Updated Security Risk Ranking

Based on general industry trend, the default security risk ranking now uses CVSS 3.0 scores as the primary score metric along with BDSA to increase vulnerability scoring accuracy.

The new default ranking is:

- BDSA (CVSS v3.x)
- NVD (CVSS v3.x)
- BDSA (CVSS v2)
- NVD (CVSS v2)

This update will only change the ranking for new installs. Any upgrades to existing instances should maintain whatever ranking order was previously set.

Version Detail Component Report Enhancement

A new **Component Link** column has been added to the Version Detail Component Report. This column will contain the component's URL as displayed when viewing the component's details page. This report is generated by selecting the desired project on the Dashboard, selecting a version, clicking the Reports tab, clicking the Create button, and then selecting Version Details Report. In the following pop-up, ensure the Component checkbox is checked to generate the components report which includes the new Component Link column.

Vulnerability Warning Display Enhancement

When viewing component vulnerabilities in your projects, Black Duck will now warn you if the vulnerability in question has a linked BDSA not associated with the version of the component used by this project version. Viewing the specified vulnerability will display a message stating one of the following messages.

In the case where a BDSA vulnerability does not have an associated NVD record:

> *The Black Duck Security Advisory (BDSA) team mapped <vulnerability ID> to this component version, but it was not included in the National Vulnerability Database (NVD)'s associated record.*

In the case where a NVD vulnerability does not have an associated BDSA record:

> *The National Vulnerability Database (NVD) mapped <vulnerability ID> to this component version, but the Black Duck Security Advisory team has determined that it is not affected.*

Please consult the Black Duck help documentation for more details on BDSA vulnerabilities.

Jobrunner Heap and CPU based throttling

Starting in Blackduck 2022.2.0, jobrunner containers will monitor their heap and CPU usage and can reduce their workload based on the current resource usage. For example, if the heap usage surpasses 90%, the jobrunner can pause itself until the memory resources have recovered. When resources become available, the jobrunner will then increase its workload in proportion to available resources.

If the jobrunner pauses itself, it will be displayed on the Admin > Diagnostics > System Information > jobruntime page. You will see an entry such as:

> 1 Active job runner endpoint(s):
>
> docker-swarm_jobrunner_1.docker-warm_default/58993e70a84c(172.23.0.15), paused=true

The `"paused=true"` indicates that this jobrunner is not taking any more work as a result of resource constraints. Once the resource utilization recovers, the entry will change to `paused=false` and the jobrunner will start to take on new work.

Ignored Snippets in the Source Report

You can now configure your environment to have ignored snippets included in your Source report. This can be done by setting the environment variable `INCLUDE_IGNORED_COMPONENTS_IN_REPORT=TRUE`.

Component Search Version Count Enhancement

You will now be able to see how many versions a particular component has when searching for components to add to your projects. The count will be dynamically displayed in the search results as you type the component name.

Security Vulnerability Remediation Enhancement

The process to remediate security vulnerabilities has been clarified to prevent confusion when attempting to change the remediation status on projects. When viewing a security vulnerability in a project, you may see rows that are hashed out and cannot be selected for remediation. This is due to the project having a linked type of security vulnerability record, either BDSA or CVE. If that vulnerability record is not prioritized in the Security Risk Ranking, a Remediation Plan cannot be undertaken for that project. Switching to the prioritized security vulnerability record will allow you to update the Remediation Plan for that project.

Project Version Cloning Enhancement

You now have the ability to include deep license data when cloning project versions. This can be done by selecting a project on your Dashboard and clicking the Settings tab when viewing the project's versions.

Search by Project Tags

You now have the ability to search and select projects by tags on the Find page. This allows the creation of saved searches for project grouped by tag - supporting dashboards for projects which could be in a common application identified by tag.

New Vulnerability Condition Rule for Policies

A new policy condition for Vulnerability IDs has been added. The new policy condition gives you the ability to create or edit a policy that allows you to target specific vulnerability (CVE or BDSA) IDs to flag components.

New Software Bill of Materials (SBOM) Report SPDX Format

You can now export the Software Bill of Materials report for your projects in SPDX format. This can be done by viewing a project version, clicking the Reports tab, and then clicking the Create Report button. We currently support SPDX 2.2 with plans to support other formats in later Blackduck versions.

Enhanced Signature Scanning Request Volume Management

In an effort to better manage higher request volumes that can occur for Enhanced Signature Scanning over a specific period of time, scan services will now return a HTTP 429 (TOO MANY REQUESTS) error that will be handled by the client if the scan services are at maximum operating limit. The client will then retry in increments of 30 seconds for 10 minutes before declaring that the scan has failed.

New Sorting Option on the Find Page

Projects can now be sorted by Project Group on the Find page, making it easier to search for projects that are assigned to specific project groups within your organization.

New projectGroupMembership filter for /api/search/project-versions

Using this filter will return all project versions that are descendant of the given project group and match conditions specified in the other filters. The `projectGroupMembership` filter will only return project groups to which the user has access. An usage example being `/api/search/projectversions?filter=projectGroupMembership:PG~{projectGroupId)`.

Report Database Enhancement

Added a new view has been added to the reporting schema:

- reporting.scan_view

Secured Communication Between Blackduck and Identity Provider (IdP)

Blackduck will now create a self signed certificate with 5 years of validity to sign SAML authentication requests. The administrator can configure whether requests require to be signed or not by going to Admin > System Settings > User Authentication, selecting SAML in the **External Authentication** section, and then checking the **Send Signed Authentication Request** checkbox.

The default setting for this option is unchecked or not required. When enabled, a link to download the Blackduck public certificate will be made available and should be distributed to your users for their IdPs to verify authentication requests.

Assigning Unmatched Components to Known Components

It is now possible to assign unmatched components found during a BOM scan to a known component.

New Rapid Scan Component Dependency Tree

We will now show the dependency tree for all instances of the vulnerable component in the project in Rapid Scans outputs. This will allow you to clearly see how that component is being referenced by other referenced components or by sub-projects, etc. An example Rapid Scan output for the `jackson-core` component with three parent dependencies:

"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"

]

],

Updated Project Group Role Names

The name for roles associated to project groups have been updated by removing the "project groups" wording. The roles' functionality have not been changed by this update. See the list below for how the roles have been updated.

- Project Group Manager → Project Manager
- Project Group Security Manager → Security Manager
- Project Group BOM Annotator → BOM Annotator
- Project Group BOM Manager → BOM Manager
- Project Group Code Scanner → Project Code Scanner
- Project Group Policy Violation Reviewer → Policy Violation Reviewer
- Project Group Viewer → Project Viewer

Project and Project Group Management Enhancements

You can now more easily add several users and project groups to projects and project groups. Dropdown menus have been enhanced to allow multiple selections in a single add user or project group interaction.

Logstash Container Memory Increase

Due to potential crashing or restarts caused by out of memory issues, we have increased the memory allocated to the Logstash container from 1024M to 2560M. This should result in fewer webapp interruptions, impacting your operations.

Project Group Deletion Enhancement

It is now no longer possible to delete a project group if it is referred to in any existing policy rule expression.

Added new extensions when searching for strings

The following extensions have been added to the list of extensions we allow to search for strings to maintain extension compatibility with FLLD/FLCD scanning in the KnowledgeBase.

- pkginfo
- properties

- pc

Supported browser versions

- Safari Version 15.0 (16612.1.29.41.4, 16612)
  - Safari versions 13.0 and below are no longer supported
- Chrome Version 94.0.4606.71 (Official Build) (x86_64)
  - Chrome versions 71 and below are no longer supported
- Firefox Version 92.0.1 (64-bit)
  - Firefox versions 71 and below are no longer supported
- Microsoft Edge Version 94.0.992.38 (Official build) (64-bit)
  - Microsoft Edge versions 78 and below are no longer supported

Container versions

- 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
- blackducksoftware/bdba-worker:2021.12.1
- blackducksoftware/rabbitmq:1.2.6

API Enhancements

For more details on new or changed API requests, please refer to the API doc available in Blackduck.

New Signed Authentication Request Field

A new `sendSignedAuthenticationRequest` field has been added to the API request below to determine whether Blackduck should send signed authentication request to IdP. The default value for this field is FALSE. The Meta link to download certificate will be available only if the Signed Authentication Request configuration is set to TRUE.

- `GET, POST /api/sso/configuration`

New /api/active-users Endpoint

This new query will return all the user last-login information for users who have logged into the system since the provided date. This query takes the same `sinceDays` query parameter as dormant-users.

New Project Version Report Endpoints

The following public endpoints have been added to support all version reports regardless of type (Notices File, Version Report, Vulnerability Remediation, Vulnerability Status, Vulnerability Update, Software Bill of Materials Report):

- `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`

New Policy Rules Public Endpoint

A new public API request has been added to retrieve active policy rules:

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

New /api/cpes/{cpeId}/origins Endpoint

With Blackduck 2022.2.0, the `/api/cpes/{cpeId}/variants` endpoint will be deprecated, to be replaced with `/api/cpes/{cpeId}/origins`. The `/api/cpes/{cpeId}/variants` will be removed in Blackduck 2022.4.0. The API link in the metadata for `/api/cpes` has also been updated to return `/api/cpes/{cpeId}/origins` instead of `/api/cpes/{cpeId}/variants`.

Page Limit Maximums on API Requests

The following API requests now have a page limit maximum in order to better moderate system resource usage. The limit is currently set to 1000 items.

- `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`

New Sorting filter for API Endpoints

A new sort option called `parentProjectGroupName` is available for the following API endpoints. This will allow for sorting project versions by parent project group name.

- `/api/search/project-versions`
- `/api/watched-projects`
- `/api/dashboards/users/{id}/saved-searches/{id}`

New GET /api/scan-readiness API Endpoint

A new public API endpoint has been added which provides the readiness state of all scan containers.

- `GET /api/scan-readiness`

Sample response:

```
{
 "readiness": "ACCEPTING",
 "items": [
  {
   "id": "9dc7653a462b",
   "service": "scan",
   "readiness": "ACCEPTING",
   "updatedAt": "2021-12-21T17:26:01.495Z",
   "versionId": 1
  }
 ]
}
```

- In a multiple scan replica environment, if all scan container replicas are healthy, the aggregated state will be `ACCEPTING`. The system can accept and process new scans without issue.
- In a multiple scan replica environment, if one scan container is not healthy and other replicas are healthy the aggregated state will be `PARTIAL`. In this state, the system is becoming overloaded. Scan performance may be degraded. Scans have a slight chance of timing out or failing.
- In a multiple scan replica environment, if all the scan containers are not healthy, the aggregated state will be `DEGRADED`. The system is overloaded cannot accept new scans. If set to reject, new scan requests will not be accepted and a HTTP 429 return code will be sent back.
- If a container goes down, its entry will be removed after 5 minutes (interval which is configurable).

Updated Response for GET /api/codelocations/{codeLocationId}/scan-summaries

The `scanType` value found in the API response generated for the `/api/codelocations/{codeLocationId}/scan-summaries` will now split into different types to avoid ambiguity. The new values now include:

- `PACKAGE_MANAGER`
- `BINARY`
- `BOM_IMPORT`
- `SIGNATURE`

Traditional scans will still use `BDIO` for `scanType` value.

Please note that this change was introduced in Black Duck 2021.8.0.

Fixed Issues in 2022.2.0

The following customer-reported issues were fixed in this release:

- (HUB-31267). Fixed an issue where users without any global roles had access to all projects via scans page or via the project URL directly. Users without scan permissions will now not see the Upload Scans button on the `projects/.../versions/.../codelocations` screen.
- (HUB-31734). Fixed an issue where the filters on the Components page did not work for project-level users.
- (HUB-31993). Fixed an issue where scans could fail if the uploaded BDIO file had a null value for version/release. Scans will no longer fail if the version/release value is missing.

- (HUB-31964). Fixed an issue where the some reports could not be generated due to VersionReportJob failing for a project-version as a result of JDBC query having too many parameters.
- (HUB-30479, HUB-31842). Fixed an issue where the remediation of vulnerabilities with both a BDSA and a CVE record did not work when the non-prioritized vulnerability record was used for remediation. In order to remediate a vulnerability, the prioritized vulnerability record type must be used.
- (HUB-31207). Fixed an issue where remediating a vulnerability under an archived project did not update the security risk counts once applied. Users cannot remediate vulnerabilities of archived project-versions, so now the "update" button for vulnerability remediations will be greyed-out when the project-version is archived.
- (HUB-32029). Fixed an issue where some "ignored" components could become "unignored" after a rescan.
- (HUB-31768). Fixed an issue when generating the notices file, copyrights based on ignored snippets were included erroneously.
- (HUB-32296, HUB-32255). Fixed an issue where REST API GET `/api/vulnerabilities/CVE-2021-44228/affected-projects` returns 0 items. Also note that the affected-projects count in both the search results and endpoint will now also count components with the related vulnerability.
- (HUB-31801, HUB-32424). Fixed an issue where the Refresh button for copyrights was appearing to the Super User role. This functionality will now only appear to roles who have the permission to update copyrights.
- (HUB-32692). Fixed an issue where if a component had multiple vulnerabilities, each with different vulnerability statuses, policy rules would not trigger a policy violation unless all vulnerabilities for the component matched the selected policy rules.
- (HUB-32357). Fixed an issue with the KnowledgeBase activity jobs that process KB Updates for components, component versions, licenses, NVD vulnerabilities, and BDSA vulnerabilities. Previously in the event of any errors/issues it would fall back to processing singular updates across all applicable project versions. This has the potential to create a lot of churn and slow down the KB Update jobs.
- (HUB-32543). Fixed an issue where the Project Manager and Project Group Manager roles could override policies and remediate vulnerabilities if the setting are turned off for the Project Manager role by assigning those roles. The security roles can now only be assigned by Project Managers with those permissions or super users.
- (HUB-31129). Fixed an issue where project versions reports in the Hub (for example the Vulnerability Detail report) would print out a URL for the vulnerabilities with CVEs containing a BDSA record if the component has a BDSA record as well. The vulnerability reports will now not print the CVE link with the BDSA number appended.
- (HUB-31044). Fixed an issue where setting the policy using the API with an incorrect custom field ID value would not display the policy screen correctly afterwards.
- (HUB-31753). Fixed an issue where the CollectScanStatsJob job could take longer than expected to compete, leading to unnecessary database bloat.
- (HUB-31663). Fixed an issue where the QuartzSearchDashboardRefreshJob could get into a condition where it tried to schedule multiple instances of this job potentially causing a large amount of blocked queries to the database.
- (HUB-31862). Fixed a missing translation for BOM Annotator Role in the Japanese localization.
- (HUB-31208). Fixed an issue where the IBM COS SDK For Java 2.10.0 component showed as vulnerable in the BOM and Component Version Security Tab, but Component Version page showed no vulnerabilities.

- (HUB-31735). Fixed an issue with snippet record discrepancies between the report (source.csv) and the Source page. The INCLUDE_IGNORED_COMPONENTS_IN_REPORT environment variable will now also drive if ignored snippets are included in a report.
- (HUB-31566). Fixed an issue where services could experience database connection errors due to job over-scheduling, out-of-memory issues, and/or long-running jobs.
- (HUB-31997). Corrected the vulnerability information for the json-schema v0.3.0 component.
- (HUB-32527). Fixed an issue when creating a Notices File Report, the following modal would display the incorrect report type name.
- (HUB-31750). Fixed broken links found on the BDSA-2021-0395 page.
- (HUB-31976). Fixed an issue where a user with 'Super User' role was unable to manage scans within the project version scans page.
- (HUB-32566). Fixed an issue where the user was unable to map a file to Apache Pulsar component.
- (HUB-31201). Fixed an issue where a user could not be assigned a user to a project (group) with only the project (group) viewer role.
- (HUB-31251). Fixed an issue where deleting a custom field option could break policy APIs.
- (HUB-29676, HUB-32912). Fixed an issue where some component versions could not be selected from the Add/Edit Component dialog box.
- (HUB-30847). Fixed an issue when the webapp container was run as a non root user, a Permission denied error was generated on the webapp-logstash pod which caused it to crash.
- (HUB-31375). Fixed an issue where the values of 'Last Updated' on Project Overview and 'Updated' on Find > Projects did not match.
- (HUB-30004). Fixed a permission issue in OpenShift environments where successful binary scans using Detect could produce blank BOMs on HUB.
- (HUB-32159). Fixed an issue where submitting an empty value for the custom signature level would generate an incorrect error message.
- (HUB-32142). Fixed an issue where RabbitMQ could fail to install on Openshift as a result of missing permissions.
- (HUB-32216). Fixed an issue when a user would try to override a policy violation for the component and the specific version then tried to undo it for the component version, nothing would happen.
- (HUB-32312). Fixed an issue where the KBUpdateWorkflow job Component Version Update would saturate and run out of memory, failing to advance the timestamp.
- (HUB-31916). Fixed an issue where the Project settings update API would not appear to take effect until the UI page was refreshed.
- (HUB-30088). Fixed an issue whereby the logout page did not appear when logging out of a SSO account.
- (HUB-32442). Fixed an issue where the API query used to retrieve dependency paths was taking significantly longer than expected to complete.
- (HUB-32538, HUB-32541). Fixed an issue where the kbUpdateJob could fail and fall back to granular updates which would take significantly longer to complete.
- (HUB-32708). Removed a statistics query introduced in Black Duck 2021.10.0 which was taking a long time to execute, causing overall slowness on Azure systems running PostgreSQL 11. This has been raised with Microsoft support, who are investigating the problem. Other installations are not affected by this issue.

- (HUB-32364, HUB-31606). Fixed an issue where the scans page could freeze and become unresponsive if there were more than 15 scans in the table and the user attempted to bulk delete them.
- (HUB-32602). Fixed an issue where the ScanPurgeJob process could erroneously cause the current scan status for package manager scans done via the IP code path to be changed to FAILED.
- (HUB-31122). Fixed an issue where sometimes scans would get skipped in the bomengine due to the ScanPurgeJob process running in the background.
- (HUB-30882). Fixed an issue where the Target Date/Actual Date of vulnerability remediation in the Report would become 1 day before than the input date due to timezone conversion.
- (HUB-32434). Fixed an issue where clicking the bell icon to show all notifications and then clicking on a project name that had generated a notification would generate an error.
- (HUB-32027). Fixed an incorrect translation for Transitive Dependency Binary for the Japanese localization.
- (HUB-30788). Added new endpoints to support all version reports regardless of types. See API Enhancements section above for additional details.
- (HUB-32843). Fixed a missing translation for "Snippets" in "Components" tab of the project version page for the Japanese localization.
- (HUB-31964). Fixed an issue where some reports could not be generated due to VersionReportJob failing for a project-version as a result of JDBC having too many parameters.
- (HUB-32393). Fixed an issue where if a snippet match was present in the BOM, the upper view would sometimes not be populated with Security/License/Operational risks if the results were filtered.
- (HUB-32604). Fixed an issue when the environment variable `BLACKDUCK_CORS_ALLOWED_ORIGINS_PROP_NAME` was set as a wildcard, the CORS functionality would not work.

Black Duck SCA 2021.10.x

Announcements for Version 2021.10.3

Security Advisory for Apache Log4J2 (CVE-2021-45046 and CVE-2021-45105)

The Apache Organization released a new version (2.17.0) of the Log4j2 component, which addresses an additional vulnerability not fixed in versions 2.15.0 and 2.16.0.

CVE-2021-45046 allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup or a Thread Context Map pattern to craft malicious input data using a JNDI Lookup pattern resulting in a denial of service (DOS) attack.

CVE-2021-45105 allows attackers with control over Thread Context Map (MDC) input data to craft malicious input data that contains a recursive lookup, resulting in a StackOverflowError that will terminate the process resulting in a denial of service (DOS) attack.

For more information, see Apache's Log4j Security Vulnerabilities page.

As stated with the Black Duck 2021.10.2 version, we believe that there is limited exposure to Black Duck' products, services and systems. To the extent we have had exposure, we have remediated or are in the process of remediating the situation. Please continue monitoring our community page for further updates.

New and Changed Features in Version 2021.10.3

Log4j Update

The Apache Log4j 2 Java library has been updated to 2.17.0 to address the critical CVE-2021-45046 and CVE-2021-45105 vulnerabilities.

Logstash Update

The Logstash image used in Black Duck has been upgraded to 7.16.2 which uses Log4j2 version 2.17.0.

Container versions

- 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
- blackducksoftware/bdba-worker:2021.9.2
- blackducksoftware/rabbitmq:1.2.5

Fixed Issues in 2021.10.3

The following issues were fixed in this release:

- (HUB-32233). Upgraded Log4j to version 2.17.0 in response to CVE-2021-45046 and CVE-2021-45105.
- (HUB-32295). Updated Bitnami Logstash to 7.16.2 version with Log4j 2.17.0.

Announcements for Version 2021.10.2

Security Advisory for Apache Log4J2 (CVE-2021-44228)

Black Duck is aware of the security issue relating to the open-source Apache Log4j 2 Java library dubbed Log4Shell (or LogJam) which was disclosed publicly via the project's GitHub on December 9, 2021. The vulnerability allows for unauthenticated remote code execution and impacts Apache Log4j 2 versions 2.0 to 2.14.1. For more information, see the official CVE posting.

Based on what we know at this time, we believe that there is limited exposure to Black Duck' products, services and systems. To the extent we have had exposure, we have remediated or are in the process of remediating the situation. Please continue monitoring our community page for further updates.

See also: https://www.blackduck.com/blog/zero-day-exploit-log4j-analysis.html

New and Changed Features in Version 2021.10.2

Log4j Update

The Apache Log4j 2 Java library has been updated to 2.15.0 to address the critical CVE-2021-44228 vulnerability.

Container versions

- 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
- blackducksoftware/bdba-worker:2021.9.2
- blackducksoftware/rabbitmq:1.2.5

Fixed Issues in 2021.10.2

The following issue wasfixed in this release:

- (HUB-32174). Upgraded Log4j to version 2.15.0 in response to CVE-2021-44228.

New and Changed Features in Version 2021.10.1

RestResponseErrorHandler Improvement

RestResponseErrorHandle now more gracefully accommodates unexpected responses from the KnowledgeBase and other servers within the network to improve the reliability of Black Duck features.

Container versions

- 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
- blackducksoftware/bdba-worker:2021.9.1
- blackducksoftware/rabbitmq:1.2.5

Fixed Issues in 2021.10.1

The following customer-reported issues were fixed in this release:

- (HUB-31129). Fixed an issue where project versions reports in the Hub (for example the Vulnerability Detail report) would print out a URL for the vulnerabilities with CVEs containing a BDSA record if the component has a BDSA record as well. The vulnerability reports will now not print the CVE link with the BDSA number appended.
- (HUB-31293). Fixed an issue where Python transitive dependencies were changed to direct dependencies after upgrading to 2021.8.x.
- (HUB-31764). Fixed an issue causing Null Pointer Exceptions during BOM computation when the remediation status of a vulnerability was updated.
- (HUB-30004). Fixed a permission issue in OpenShift environments where successful binary scans using Detect could produce blank BOMs on HUB.
- (HUB-31879). Fixed an issue where scans could get stuck during the building bom phase. See the RestResponseErrorHandler improvement in the New and Changed Features section above for more details.
- (HUB-31896). Fixed an issue where remediation updates to BOM vulnerabilities via public api did not persist after re-scan.
- (HUB-31753). Fixed an issue where the CollectScanStatsJob job could take longer than expected to compete, leading to unnecessary database bloat.

- (HUB-31663). Fixed an issue where the QuartzSearchDashboardRefreshJob could get into a condition where it tried to schedule multiple instances of this job potentially causing a large amount of blocked queries to the database.
- (HUB-31755). Fixed an issue when generating a Project Version report that could cause VersionReportJob to run out of memory due to cyclic project structure.
- (HUB-31566). Fixed an issue where services could experience database connection errors due to job over-scheduling, out-of-memory issues, and/or long-running jobs.

Announcements for Version 2021.10.0

Enhanced Signature Scanning

The same performance improvements that were introduced to Package Manager Scanning in the 2021.8.0 release are available in the 2021.10.0 release for Signature Scanning. A key part of these improvements is Duplicate BOM Detection. With this feature, if a Signature Scan will not alter the BOM already associated with the specific Project and Version, then BOM Computation is bypassed.

Additionally, with Enhanced Signature Scanning the JobRunner no longer plays a role in processing of incoming Package Manager or Signature Scans. Although more system resources are not required to run Enhanced Signature Scans, it is possible that minor rebalancing of the containers is required. Please reach out to Black Duck support who can help you understand if any rebalancing is needed. We encourage all our customers to do so and take advantage of these improved capabilities.

Clarification on Detect 7.4 with Black Duck 2021.8.0

In order to ensure full functionality and compatibility, Black Duck version 2021.8.0 requires Detect 7.4. Users can continue to use older versions of Detect with Black Duck, but may encounter inaccurate dependency types or source views in the BOM when using aggregated BDIO files.

Upgrading to Detect 7.4 will ensure you avoid these inaccuracies in the BOM.

PostgreSQL container migration from 9.6 to 11

Black Duck will migrate its PostgreSQL image from version 9.6 to version 11 with the **2022.2.0** release. Customers not using the Black Duck-supplied PostgreSQL image will not be affected.

Black Duck PostgreSQL 9.6 deprecation

As announced in the Black Duck 2020.6.0 release, Black Duck was to end support for external PostgreSQL 9.6 for the 2021.6.0 release. Starting with the **2022.2.0** release, Black Duck will no longer work with PostgreSQL 9.6 and will fail to start if pointed to a PostgreSQL 9.6 instance.

PostgreSQL support schedule

Starting with the upcoming **2022.10.0** release, Black Duck will end support for external PostgreSQL 11. Please see the table below for the projected dates for the beginning and end of support for future PostgreSQL versions.

PG Version	First Release	Last Release	BD External Support Added	BD External Support End
16.x	Late 2023	Late 2028	2024.10.0	2026.10.0
15.x	Late 2022	Late 2027	2023.10.0	2025.10.0
14.x	September 2021	November 2026	2022.10.0	2024.10.0

13.x	September 2020	November 2025	2021.8.0	2023.10.0
12.x	October 2019	November 2024	X	X
11.x	October 2018	November 2023	2020.6.0	2022.10.0

Database bds_hub_report deprecation starting with 2021.10.0

Starting with 2021.10.0, new installations of Black Duck will no longer create the `bds_hub_report` database. We plan to finally delete `bds_hub_report` in 2022.10.0.

Also, the `hub_create_data_dump.sh` and `hub_db_migrate.sh` scripts (which are distributed with our orchestration files) will no longer fail if `bds_hub_report` does not exist.

- The `hub_create_data_dump.sh` script will dump `bds_hub_report` if it exists but will not fail if it doesn't. If `bds_hub_report` is absent, the script will print a message saying it was skipped.
- The `hub_db_migrate.sh` script will try to restore `bds_hub_report` if it exists, regardless of whether or not a dump file is present (matching the behavior of prior releases). If `bds_hub_report` is not present, it will not try to restore it, also regardless of whether or not a dump file is present.
- A new script, `hub_recreate_reportdb.sh` is added to recreate `bds_hub_report` if a user wants propagate their `bds_hub_report` DBs from 2021.8.x or earlier to a new install of 2021.10.0 or later. In this case;
  - Run `hub_create_data_dump.sh` on the old BD instance.
  - Run `hub_recreate_reportdb.sh` on the new BD instance.
  - Run `hub_db_migrate.sh` on the new BD instance with the dumps created in step #1.

Upcoming max page limit enforcement for API requests

Starting with Black Duck **2022.2.0**, max page limits on API requests will be enforced. Users should make singular requests that include a limit request parameter smaller or equal to the documented page limit. Requests for pages greater than the documented limit will be truncated to only return the maximum accepted page limit. Requests for page sizes will not be rejected but return a maximum number of results per paged request.

This will be an ongoing effort lasting subsequent releases to improve application stability and prevent performance degradation from unreasonably large requests.

Deprecated APIs

The following defunct endpoints will now return a 404 NOT FOUND error to indicate that access to the target resource is no longer available:

- GET /oauthclients
- POST /oauthclients
- DELETE /oauthclients/{oAuthClientId}
- GET /oauthclients/{oAuthClientId}
- PUT /oauthclients/{oAuthClientId}
- POST /vulnerabilities/vulndb-copy

Japanese language

The 2021.8.0 version of the UI, online help, and release notes has been localized to Japanese.

Simplified Chinese language

The 2021.8.0 version of the UI, online help, and release notes has been localized to Simplified Chinese.

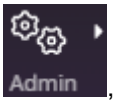
New and Changed Features in Version 2021.10.0

Updated error messages for the Enhanced Signature Generation

Signature scanning server-side error messages have been updated. A complete list of error messages will be made available in the user guide in an upcoming release.

Unmapped scans data retention configuration setting

A new configuration setting is now available for administrators to change the default retention period for unmapped scans. Starting with Black Duck 2021.10.0, this setting will be enabled by default and set to a period of 30 days (previously 365 days). This retention setting can be updated and set to as low as 1 day and to as high as 365 days.

To change this setting in the UI, click 

, click Settings, and then click Data Retention.

Estimated Security Risk

This estimated risk statistic is formulated by looking at all the versions of a component sorted by security vulnerability severity category and calculating the maximum vulnerability count for each severity category for each component version. The maximum vulnerability count for each severity category is shown in the “Estimated Security Risk by Severity Category" on the Bill of Material for Security risk. The highest severity category counts may reference different component versions. For example:

- Version 1.1 has 2 Critical, 3 High, 15 Medium, 4 Low
- Version 1.2 has 2 Critical, 4 High, 12 Medium, 1 Low
- Estimated Security Risk by severity category for components with unknown versions would return as 2 Critical, 4 High, 15 Medium, 4 Low on the BoM.

Users should choose the exact version used in the application to view the accurate risk instead of the estimated risk. This estimated risk information is provided to help prioritize what components to review first. Users are encouraged to use estimated risk information in conjunction with BD Policy Management to further prioritize what components to triage first based on their company’s security policies.

Note: The information presented is only a statistical data estimation. As a result, the estimated security risks will not have CVE data.

Generating Notices report when deep license data is enabled

The notices file will now place any declared licenses before additional ones. The declared and additional licenses will then be sorted alphabetically.

Addition of comments to the Source view and the Source report

Comments can now be added to entries in the Source view of a project. File comments are also shown in the snippet view. These comments also appear in the Source Report in the new column labeled Comments. Select the Source check box for the Version Detail Report in the Report tab to create a Source Report.

You can leave a comment for a particular entry in the Source tab by:

- clicking the icon found at the end of that component's row and selecting Comments from the dropdown menu or clicking the icon if there are already comments present.
- clicking the entry in the Source view, clicking the Name of the component, clicking the icon, and then selecting Comments from the dropdown menu or by clicking the icon if there are already comments present.

Policy Management Enhancement - Project Groups

Black Duck users will now have the ability to apply policy rules to project group(s) and its descendants. To do so, go to **Policy Management** and either click the **Create Policy Rule** button or the button and select **Edit**. When the Create/Edit Policy Rule modal opens, ensure the **A Subset of Projects, filtered by...** option is enabled to see the Project Conditions filter dropdown.

Policy Management Enhancement - Added (RCE) Remote Code Execution to Vulnerability Conditions

Black Duck users will now have the ability to add Remote Code Execution (RCE) as a filter option when creating or editing policies. To do so, go to **Policy Management** and either click the **Create Policy Rule** button or the button and select **Edit**. The new (RCE) Remote Code Execution value will be displayed in the Vulnerability Conditions dropdown menu.

Changes to Project Group Manager permissions

Previously, the actual permissions of the Project Group Manager were not affected by the global settings for allowing a project manager to remediate vulnerabilities or override policy. Now, the Project Group Manager role permissions will be adjusted based on Project Manager Role Settings.

Signature scanner dry run update

Previously, when performing a Signature Scanner dry run, the output would produce a JSON file. Starting with Black Duck 2021.10.0, the produced output file will be a .bdio extension, and is a zip file. It will continue to be generated in the same directory as dry run as traditional signature scanning.

Supported browser versions

- Safari Version 15.0 (16612.1.29.41.4, 16612)
  - Safari versions 13.0 and below are no longer supported
- Chrome Version 94.0.4606.71 (Official Build) (x86_64)
- Firefox Version 92.0.1 (64-bit)
- Microsoft Edge Version 94.0.992.38 (Official build) (64-bit)
  - Microsoft Edge versions 79 and below are no longer supported

Container versions

- 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
- blackducksoftware/bdba-worker:2021.9.1
- blackducksoftware/rabbitmq:1.2.5

API Enhancements

Permission fixes to GET /api/project-groups

The following fixes have been made to the `GET /api/project-groups` api endpoints:

- `GET api/project-groups` will only return the project groups the user is authorized to view as search results.
- `GET api/project-groups/<project group ID>` will return a HTTP 200 OK for users with the Super User role or a HTTP 403 FORBIDDEN response otherwise.

Permission changes to GET /api/users/{userId}

The `GET /api/users/{userId}` endpoint now no longer has a permission check (previously required a USERMGMT_READ check).

- The `GET /api/users/`endpoint (that lists all users) will continue to be protected with the USERMGMT_READ permissions.
- The projectOwner user (regardless of the user's permission status) in the `/api/projects/{projectId}` API will still be provided.
- The USERMGMT_READ permission that was added to project roles in Black Duck version 2021.8.2 will still be removed.

New filter parameter for GET /api/project-groups

A new filter parameter called `exactName` has been added to help find specific project groups. When true, the `exactName` filter will ensure only the project group that matches the name value in `q` is returned. The search criteria for the project group is case-insensitive. If none match, then nothing is returned. Also, the `q` parameter must be specified when the `exactName` filter is true otherwise no project groups will be returned.

See below for how the filter is used in a `/api/project-groups` request:

```
/api/project-groups?q=name:<project group name>&filter=exactName:true
```

Improved CPE Support APIs

Three new public APIs have been added:

- `GET /api/cpes` [Requires a searchParam. Returns matching CPE IDs]
- `GET /api/cpes/{cpeId}/versions` [Returns component-versions matching the CPE ID]
- `GET /api/cpes/{cpeId}/variants` [Returns component-origins matching the CPE ID]

Copyright 2.0 data and new legacy endpoint

Black Duck is now rolling out Copyright 2.0 data using the existing endpoint (below) to serve this new copyright data. No response fields are being dropped or added.

```
GET /api/components/{componentId}/versions/{componentVersionId}/origin/{originId}/file-copyrights
```

We will continue to serve Copyright 1.0 (aka legacy) data by creating a new endpoint :

```
GET /api/components/{componentId}/versions/{componentVersionId}/origin/{originId}/file-copyrights-legacy
```

Note: This new endpoint is not directly used in Black Duck UI, only through the public API directly. Also, since the existing endpoint will now return Copyright 2.0 data, all Black Duck customers (regardless of the version they use) should see this new data.

Exposure of lastScanDate through a Public API

The following API will now expose `lastScanDate` in the Public API response:

- `GET /api/projects/{projectId}/versions/{projectVersionId}/bom-status`

Fixed Issues in 2021.10.0

The following customer-reported issues were fixed in this release:

- (HUB-29413). Searching for components in the Add Component or Edit Component modals is now more accurate, and Custom Components are more easily found.
- (HUB-26545 and HUB-30185). Fixed an issue where the following Public REST API endpoints did not update the componentModification, componentModified, and componentPurpose component conditions as expected.
  - `/api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}`
  - `/api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}`
- (HUB-30474). Fixed an issue where the count displayed on the Affected Projects page was not matching the actual results when the user has no access to certain projects.
- (HUB-30623). Fixed issues where a number of client-initiated errors were creating heavy log churn via logging of stacktraces or were incorrectly logged at a more severe log level than they actually represented.
- (HUB-30099). Fixed an issue where Vulnerability statuses were not updated for existing BOMs by KB update. BoM Component-Version Vulnerability remediations (found in the BoM-security view) will now be updated by the KB Update Job when the remediation status changes if the current status is not user or system updated.

- (HUB-29773). Fixed an issue where the `/api/projects/<project ID>/versions/<version ID>/vulnerable-bom-components` endpoint would have longer than expected response times. The request now only includes one license definition per version BOM component which should improve the response time. Users should only see a lower number of results if they had a Protex BOM imported with license overrides.
- (HUB-26924). Fixed an issue so that a user-friendly error message now appears when a SAML SSO user login fails. If the SSO configuration is wrong, an error page will be displayed to indicate a configuration issue. If the user is disabled in HUB, an error page will be displayed, notifying the user to contact the system administrator or Unauthorized page.
- (HUB-31176). Fixed an issue where Rapid Scan policy evaluation was not checking the BOM status when the remediation status is associated with a specific project-version.
- (HUB-30808). Fixed an issue where custom fields created under the BOM Component tab in Custom Fields Management were not returning when reviewing a component's "Additional fields" within any project's BOM. We will display up to 100 custom fields when editing the custom fields on BOM component.
- (HUB-30922). Fixed an issue where the descriptions on the Project Version level were not displayed. This field will now display the description used on the Project level.
- (HUB-31482). Fixed an issue where licenses were not shown on the Snippet confirmation page after HUB 2021.6.2.
- (HUB-31003). Fixed an issue where users could get a HTTP 500 Internal Server Error when attempting to perform bulk remediation for vulnerabilities.
- (HUB-31425). Fixed an issue where the Version Detail Report was taking a significant amount of time to run/complete the query when started compared to previous versions of HUB.
- (HUB-29598). Fixed an issue where the number of vulnerabilities in the PDF generated by "Print" button on component page would get pushed out due to the bar being too long.
- (HUB-30133). Fixed an issue where the t-shirt sizing ymls in the helm deployments have the webui container with less memory for an XL deployment than large. The webui container's memory limit is increased to 1024 Mi in x-large.yaml tshirt size.
- (HUB-28889). Fixed an issue where the BOM Engine could fail to start if RabbitMQ is not reachable.
- (HUB-30215). Fixed an issue where BDSA-2020-1311 was incorrectly reporting a workaround was available.
- (HUB-30857). Fixed a bug where the "Affected Projects" page for vulnerabilities was omitting vulnerabilities from ignored components in the items displayed but including them when finding the count for the total items. Now the count for total items also omits vulnerabilities from ignored components.
- (HUB-30603). Fixed an issue where a user could see the entirety of a comment under a BDSA or CVE record under the security tab of a project if it was grayed out.
- (HUB-28753). Fixed an issue where the BomEngine did not accept the value of the HUB_PROXY_PASSWORD_FILE secret when created in docker and would return a 407 AUTHENTICATION REQUIRED error.
- (HUB-31483). Fixed an issue where the policy override date and user information in the Policy Violations modal was displayed incorrectly the Japanese localization.

Black Duck SCA 2021.8.x

New and Changed Features in Version 2021.8.8

Black Duck version 2021.8.8 is a maintenance release and contains no new or changed features. A fix was made to the online help to address CVE-2022-30278 which could allow an unauthenticated remote attacker to conduct a cross-site scripting attack.

Container versions

- 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
- blackducksoftware/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

Fixed Issues in 2021.8.8

The following customer-reported issues have been fixed:

- (HUB-32811). Fixed an issue where some reports could not be generated due to VersionReportJob failing for a project-version as a result of JDBC having too many parameters.

Announcements for Version 2021.8.7

Security Advisory for Apache Log4J2 (CVE-2021-45046 and CVE-2021-45105)

The Apache Organization released a new version (2.17.0) of the Log4j2 component, which addresses an additional vulnerability not fixed in versions 2.15.0 and 2.16.0.

CVE-2021-45046 allows attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup or a Thread Context Map pattern to craft malicious input data using a JNDI Lookup pattern resulting in a denial of service (DOS) attack.

CVE-2021-45105 allows attackers with control over Thread Context Map (MDC) input data to craft malicious input data that contains a recursive lookup, resulting in a StackOverflowError that will terminate the process resulting in a denial of service (DOS) attack.

For more information, see Apache's Log4j Security Vulnerabilities page.

As stated with the Black Duck 2021.8.6 version, we believe that there is limited exposure to Black Duck' products, services and systems. To the extent we have had exposure, we have remediated or are in the process of remediating the situation. Please continue monitoring our community page for further updates.

New and Changed Features in Version 2021.8.7

Log4j Update

The Apache Log4j 2 Java library has been updated to 2.17.0 to address the critical CVE-2021-45046 and CVE-2021-45105 vulnerabilities.

Logstash Update

The Logstash image used in Black Duck has been upgraded to 7.16.2 which uses Log4j2 version 2.17.0.

Container versions

- 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
- blackducksoftware/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

Fixed Issues in 2021.8.7

The following issues have been fixed:

- (HUB-32233). Upgraded Log4j to version 2.17.0 in response to CVE-2021-45046 and CVE-2021-45105.
- (HUB-32295). Updated Bitnami Logstash to 7.16.2 version with Log4j 2.17.0.

Announcements for Version 2021.8.6

Security Advisory for Apache Log4J2 (CVE-2021-44228)

Black Duck is aware of the security issue relating to the open-source Apache Log4j 2 Java library dubbed Log4Shell (or LogJam) which was disclosed publicly via the project's GitHub on December 9, 2021. The vulnerability allows for unauthenticated remote code execution and impacts Apache Log4j 2 versions 2.0 to 2.14.1. For more information, see the official CVE posting.

Based on what we know at this time, we believe that there is limited exposure to Black Duck' products, services and systems. To the extent we have had exposure, we have remediated or are in the process of remediating the situation. Please continue monitoring our community page for further updates.

See also: https://www.blackduck.com/blog/zero-day-exploit-log4j-analysis.html

New and Changed Features in Version 2021.8.6

Log4j Update

The Apache Log4j 2 Java library has been updated to 2.15.0 to address the critical CVE-2021-44228 vulnerability.

Container versions

- 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
- blackducksoftware/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

Fixed Issues in 2021.8.6

The following issues have been fixed:

- (HUB-32174). Upgraded Log4j to version 2.15.0 in response to CVE-2021-44228.

New and Changed Features in Version 2021.8.5

Black Duck version 2021.8.5 is a maintenance release and contains no new or changed features.

Container versions

- 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
- blackducksoftware/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

Fixed Issues in 2021.8.5

- (HUB-31482). Fixed an issue where licenses were not shown on the Snippet confirmation page after Black Duck version 2021.6.2.
- (HUB-31663). Fixed an issue where the QuartzSearchDashboardRefreshJob could get into a condition where it tries to schedule multiple instances of this job causing a large amount of blocked queries.

New and Changed Features in Version 2021.8.4

Black Duck version 2021.8.4 is a maintenance release and contains no new or changed features.

Container versions

- 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
- blackducksoftware/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

Fixed Issues in 2021.8.4

- (HUB-31425). Fixed an issue where the Version Detail Report was taking a significant amount of time to run/complete the query when started compared to previous versions of HUB.

New and Changed Features in Version 2021.8.3

Reporting database enhancements

Added the following data to scan_stats_view under the reporting schema:

- scan_size

Container versions

- 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

- blackducksoftware/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

Fixed Issues in 2021.8.3

The following customer-reported issues were fixed in this release:

- (HUB-29959, HUB-30391, and HUB-30397). Fixed an issue where scans would not complete due to a 500 Internal Error response from the KnowledgeBase while preparing the Bill of Materials.
- (HUB-31047). Fixed an issue when populating the version BOM components page, the UI makes duplicate calls to the back-end generating unnecessary stress to the database.
- (HUB-30074). Fixed an issue where very small code locations snippet scans sometimes finish before upload source info is updated giving the appearance that the uploaded source was lost.

New and Changed Features in Version 2021.8.2

Black Duck version 2021.8.2 is a maintenance release and contains no new or changed features.

Container versions

- 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
- blackducksoftware/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

Fixed Issues in 2021.8.2

The following customer-reported issues were fixed in this release:

- (HUB-31078). Documented an issue where install and upgrade to Black Duck 2021.8 would fail in Kubernetes when the `--reuse-values` flag is used as part of the installation/upgrade. Please refer to the REAME.md under Helm charts for more details.

- (HUB-31086). Fixed an issue where the snippets box at top right side of BOM Page was missing for few project versions.
- (HUB-31156). Fixed an issue where users with the Project level BOM Manager role and without any Global or Overall roles would not able to access the Project BOM.

New and Changed Features in Version 2021.8.1

Black Duck version 2021.8.1 is a maintenance release and contains no new or changed features.

Container versions

- 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
- blackducksoftware/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

Fixed Issues in 2021.8.1

The following customer-reported issues were fixed in this release:

- (HUB-31029). Fixed an issue where the Project Manager Role settings was overriding the individual/ group's Super User role.
- (HUB-30808). Fixed an issue where custom fields created under the BOM Component tab in Custom Fields Management were not returning when reviewing a component's "Additional fields" within any project's BOM.
- (HUB-30655). Fixed an issue where users without the Super User role could see "Project Group Management" option in the Management menu.
- (HUB-31077). Fixed an issue where upgrading Black Duck HUB from 2021.6.0 to 2021.8.x would fail for Kubernetes deployments due to a change made to a property in the helm chart. Other prior versions are unaffected.

Announcements for Version 2021.8.0

Detect 7.4 required for Black Duck 2021.8.0 release

Black Duck version 2021.8.0 requires Detect 7.4 in order to run. Please ensure you meet this minimum version requirement when upgrading.

Desktop Scanner on CentOS-7

As a result of updated dependencies, the latest version of Desktop Scanner will not run on CentOS-7. Therefore, a different RPM was created specifically for the CentOS-7 build which will be running with an older version of Electron 12. We will maintain this separate CentOS-7 build for as long as Electron 12 is supported.

In addition to our current downloads, a link has been added on the Tools page specifically for the CentOS-7 download. The regular RPM, debian package, macOS and Windows installers are available as usual.

Japanese language

The 2021.6.0 version of the UI, online help, and release notes has been localized to Japanese.

Simplified Chinese language

The 2021.2.0 version of the UI, online help, and release notes has been localized to Simplified Chinese.

Deprecated APIs

The following endpoint has been removed:

- GET /api/scan/{scanId}/bom-entries

The following defunct endpoints will now return a 410 GONE error to indicate that access to the target resource is no longer available:

- GET /oauthclients
- POST /oauthclients
- DELETE /oauthclients/{oAuthClientId}
- GET /oauthclients/{oAuthClientId}
- PUT /oauthclients/{oAuthClientId}
- POST /vulnerabilities/vulndb-copy

New and Changed Features in Version 2021.8.0

PostgreSQL 13 support for external databases

Black Duck now supports and recommends PostgreSQL 13 for new installs that use external PostgreSQL. Migrating to 2021.8.x does not require migration to PostgreSQL 13.

No action is required for users of the internal PostgreSQL container.

Please note that PostgreSQL 12 is not supported.

Installation documentation will be updated in an upcoming release.

Notice for Azure customers

Support for Black Duck on Azure PostgreSQL 13 will be best-effort only with no guarantee of resolution until Azure PostgreSQL 13 is fully released. As such, we very strongly recommend against using Azure PostgreSQL 13 for production deployments and customer should use Azure PostgreSQL 11.

For more information on Azure support for PostgreSQL 13, please visit https://docs.microsoft.com/en-us/azure/postgresql/concepts-version-policy.

New System Setting for scans: Component Dependency Duplication Sensitivity

This setting allows users to change how the system displays duplicate package ID's for components on the Source page that are found during scans. In previous releases and as the default setting in 2021.8.0 (set to 1), the Source page will only display one package ID discovery regardless of how often it is found in your scan. Changing this setting to greater than 1 will display more entries allowing for greater layer-by-layer insight to help determine from which layer each component originated. This feature is especially useful to customers who are scanning in Detect with BOM aggregation enabled and want to see package ID references across the various modules that have been aggregated into 1 scan.

New System Setting for scans: Minimum Scan Interval

This setting allows users to change the minimum hourly frequency of which signature scans can be performed for a given code location when using the LCA enhanced signature scanning. The default setting is set to 0, or no minimum scan interval, meaning scans are not prevented from occurring regardless of frequency. If set to greater than 0, signature scans will not be processed if they occur before the set scan interval. For example, a setting of 4 will not allow signature rescans before 4 hours of time have elapsed. This setting may be configured globally in the Administration > System Settings > Scan page or through the Detect client as a command line option. Note: This setting is only used if customer scan using the parameter --detect.blackduck.signature.scanner.arguments='--signature-generation'.

Note: When this feature is enabled, signature scans with Detect will finish with a status of success even if the signature scan was not run due to the scan interval. A warning message will appear in the logs indicating the scan was not run, but there will be no other indication given to the user.

Changes in Rapid Scan policy application

Rapid Scan users now have the ability to configure how policies are applied to the results of Full (traditional) scans, Rapid Scans, or both. The default setting for new installations of Black Duck starting from version 2021.8.0 will be set to apply to full scans only. To use Rapid Scan to fetch all vulnerabilities regardless of policies, simply create a single policy, setting the condition severity >=0.

Added phone-home cumulative count of the number of rapid scans done

This count is accurate and data is not lost, but there might be some timing issues where some of the scans are from the subsequent day’s data.

Rapid Scan vulnerability conditions added to Policy Management

The following vulnerability conditions are now available in Policy Management:

- CWE IDs
- Solution Available
- Workaround Available
- Exploit Available
- Reachable from Source

- Remediation Status

Project Group Management

Black Duck now provides the ability to logically group all your projects in the Hub, allowing you to organize which projects belong to which business unit making it easier for you to view risk across the organization. Project groups can contain both projects and other project groups to provide a multi-level hierarchy.

Users and Groups can be assigned to Project Groups with any number of roles. That assignment will give those users access to the projects below that group with the specified roles unless that assignment is explicitly overridden at the lower levels. This concept allows for setting users with default access to projects that haven't been created yet.

In addition, the search dashboard has been enhanced to return search results for projects the user has access to via a project group.

New Global Release Creator, Project Group BOM Annotator user roles, and changes to existing roles

The Project Creator and Global Code Scanner roles have had their access to the Global Release Create permission revoked and will no longer be able to create releases of projects they do not own or have access to. A new role, Global Release Creator, has been made to fill in the gap for users who depended on this functionality. All current users with Project Creator and/or Global Code Scanner will automatically inherit this role as part of the upgrade migration script. That means this change will be specifically opt-out for current users looking to take advantage of the more narrow security change.

The Project Group BOM Annotator has the BOM Annotator permissions for every project in the assigned project group. This means they can add or edit comments and edit custom fields for projects associated with the project group.

Protex BOM Tool token access support enhancement

The Protex BOM tool now supports the BD_HUB_TOKEN environment variable to upload json exported from Protex to the Hub. You can set the token by adding "-T " using command prompt.

Add `BD_HUB_TOKEN=[insert token here]` variable to `.bash_profile` to make the change permanent.

Vulnerability Notifications enhancement

Added a new environment variable: `BLACKDUCK_NOTIFY_WHEN_REMEDIATED` in the `blackduck-config.ev` file. It defaults to true, but when set to false Black Duck will no longer send/create "new" vulnerability notifications for vulnerabilities with a remediation status of "Ignored, Remediation Complete, Mitigated, or Patched."

Signature scan timeout message enhancement

Network timeouts during a signature scan (waiting for a response from HUB) now return an accurate error message that indicates a network timeout and not an I/O error (code 74). The new message format will display `Scan <Corresponding Scan ID> failed: [<Reason why it happened and whether to contact an administrator or retry the scan>]`.

Request Retry mechanism for Black Duck Hub enhancement

A waiter has been introduced which will retry uploading the scan to Hub when it receives HTTP 502/503/504 responses. It will retry in increments of 30 seconds for 10 minutes before declaring that the scan is failed.

Scans page enhancement

A new Created column was added to the Scans page allowing you to see when the scan was created. The date displayed in the column with make it easier to compare dates when filtering scans using the Created Date option.

Surface license risk info for Components without versions

New logic has been introduced to determine a default license for components with an unknown version. This is an estimated license based on greatest number of times it shows up across the top 1,000 versions of the component. With this, you will be able to calculate license risk without requiring a version to be selected. It is, however, recommended that you review these components and manually specify a version for more accurate results.

Reporting database enhancements

Added the following data to scan_stats_view under the reporting schema:

- 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

Policy rule condition enhancement

A new policy condition operator was added for policy rules Vulnerability Conditions Category for Overall Score. You may now select "Less than or equal to" when creating or editing policy rules.

Container versions

- 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
- blackducksoftware/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

API enhancements

- New API added that enables bulk confirm/un-confirm ignore/un-ignore of snippet matches.
  - `PUT /api/projects/{projectId}/versions/{versionId}/bulk-snippet-bom-entries Media Type: application/vnd.blackducksoftware.bill-of-materials-6+json`
- The following API endpoints have been updated to consider projects the user can access via project group membership. The query parameter has also changed from `name` to `entityName` for parity with the response content.
  - `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`

Fixed Issues in 2021.8.0

- (HUB-29341). Fixed an issue when exporting BOM from Protex using the --include-files flag and then importing it to a Hub instance would generate a Java heap space error.
- (HUB-29005). Fixed an issue where if a BOM has two components with the exact same name but different UUIDs, the filter API (`/api/projects/projectId/versions/versionId/components-filters?filterKey=bomComponents`) should return two separate components based on ID and their versions (if present) rather than grouping them by name.
- (HUB-29567). Fixed an issue where the “Updated” (or “Last Settings Update” in 2021.8.0) timestamp would be updated but not the updated by user name on the Project version > Details view. The “Last Settings Update” timestamp and updated by user name will now only be updated when project version details are changed.
- (HUB-30139). Fixed an issue in the Protex BOM tool where an Unmarshalling Error: Illegal character occurred when using the --include-files flag.

- (HUB-12280). Fixed an issue where uploading a bdio file with relationships to the project are not visible when they are also located lower in the 'bdio tree'.
- (HUB-29481). Fixed an issue where licenses with the same name but different capital letters were being omitted from notices reports.
- (HUB-30143). Fixed an issue where the Protex BOM tool 2021.6.0 did not work with latest JDK (11.0.11).
- (HUB-29274). Fixed an issue where VersionReportJob could cause jobrunner Out Of Memory issue when there are circular references on BOM page.
- (HUB-29381). Fixed an issue when a project version is added as a component (using Add > Project), the component entry would show an invalid Operational Risk level.
- (HUB-30087). Fixed an issue where the project version query fails to find the version when version name includes multi-byte alpha-numeric characters.
- (HUB-23686). Fixed an issue when running Detect against a node file the signature scanner would get stuck.
- (HUB-25592). Fixed an issue where component (or component version)'s adjustments got dropped automatically from BOM.
- (HUB-25552). Fixed an issue where component (or component version) with 'MATCH' type adjustments were automatically added/deleted from BOM.
- (HUB-29196). Fixed an issue where the policy violation pop-up did not disappear when it was clicked and the mouse cursor was moved away from the policy violation symbol quickly.
- (HUB-29573). Fixed an issue where line breaks in a policy rule's description were ignored when viewing the policy violation modal.
- (HUB-30611). Fixed an issue with where numeric usernames were causing errors in a database migration script.
- (HUB-26611). Fixed an issue where Direct/Transitive dependencies were not reported correctly when using aggregation in Detect. Please note that this fix is resolved only when using Detect 7.4 and requires using the new SUBPROJECT `detect.bom.aggregate.remediation.mode` in Detect.
- (HUB-22379). Fixed performance issues where project tagging and having tag policy can take hours on some instances.
- (HUB-30141). Fixed an issue with Hub swarm docker-compose.yml containing the unsupported "links" options.
- (HUB-29549). Fixed a performance issue with the loading of the BOM page caused by permission checks.

Black Duck SCA 2021.6.x

New and Changed Features in Version 2021.6.2

Black Duck version 2021.6.2 is a maintenance release and contains no new or changed features.

Container versions

- 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
- blackducksoftware/bdba-worker:2021.06
- blackducksoftware/rabbitmq:1.2.2

Fixed Issues in 2021.6.2

The following customer-reported issues were fixed in this release:

- (HUB-30493). Fixed an issue where the Blackduck Alert instance was not accessible for hosted users due to specifying the proxy certificate location for Alert in NGINX configuration.

New and Changed Features in Version 2021.6.1

Black Duck Security Advisory (BDSA) Remote Code Execution Exposure

Black Duck highlights vulnerabilities that may allow Remote Code Execution (RCE) in the 2021.6.1 release. In the Black Duck UI, if the BDSA vulnerability has a RCE tag it will appear in the full BDSA record, the table of vulnerabilities, and in the Security tab of a particular component.

The vulnerability APIs report the vulnerability using an array with the name bdsaTags. If the bdsaTag array includes “RCE” then that vulnerability may allow Remote Code Execution.

- /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

Container versions

- 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
- blackducksoftware/bdba-worker:2021.06
- blackducksoftware/rabbitmq:1.2.2

Fixed Issues in 2021.6.1

The following customer-reported issues were fixed in this release:

- (HUB-29202). Fixed an issue where the binary scan container(bdba-worker) of 2021.4.0 did not work on docker SWARM by increasing timeout and retry values.
- (HUB-29405). Fixed an issue where matches were being dropped, due to the identification of a core_i7 architecture.
- (HUB-30134). Fixed an issue where the BOM engine silently fails to start due to RabbitMQ connectivity issue.
- (HUB-30170). Fixed an issue where Redis fails to start due to incorrect configuration in the docker-entrypoint when utilizing dual stack Kubernetes.
- (HUB-30202). Fixed an issue where the vulnerability details page does not correctly change the display of the score metrics when the user clicks from BDSA scoring to NVD scoring and vice versa.

Announcements for Version 2021.6.0

Support ending for PostgreSQL version 9.6 for external databases

As of the Black Duck 2021.6.0 release, Black Duck has ended support for PostgreSQL version 9.6 for external databases.

Black Duck will now only support PostgreSQL version 11.x for external databases.

Deprecated page

As announced previously, the Scans > Components page has been removed.

Deprecated APIs

The following endpoints have been deprecated:

- GET /oauthclients
- POST /oauthclients
- DELETE /oauthclients/{oAuthClientId}
- GET /oauthclients/{oAuthClientId}
- PUT /oauthclients/{oAuthClientId}
- POST /vulnerabilities/vulndb-copy

Japanese language

The 2021.4.0 version of the UI, online help, and release notes has been localized to Japanese.

New and Changed Features in Version 2021.6.0

New containers and changes to system requirements

In the 2021.6.0 release:

- A new container, blackduck-webui, has been added for improved Black Duck performance, better caching, and future scalability.
- The Rapid Scanning feature is now available to all Black Duck customers. This feature requires a new container, blackduck-matchengine, which manages connections to the Black Duck KnowledgeBase and cache KnowledgeBase results for short intervals.

The following are now the minimum hardware that will be needed to run a single instance of all containers. Note that memory requirements depend on the number of concurrent Rapid Scans you want to support.

- 7 CPUs
- 28.5 GB RAM for the minimum Redis configuration; 31.5 GB RAM for an optimal configuration providing higher availability for Redis-driven caching. This will support up to 100 concurrent Rapid Scans.

  30 GB RAM for the minimum Redis configuration; 33 GB RAM for an optimal configuration providing higher availability for Redis-driven caching. This will support more than 150 Rapid Scans, however, the maximum number of supported Rapid Scans is still being determined.
- 250 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

The following is the minimum hardware that is needed to run Black Duck with Black Duck Binary Analysis.

- 8 CPUs
- 32.5 GB RAM for the minimum Redis configuration; 35.5 GB RAM for an optimal configuration providing higher availability for Redis-driven caching. This will support up to 100 concurrent Rapid Scans.

  34 GB RAM for the minimum Redis configuration; 37 GB RAM for an optimal configuration providing higher availability for Redis-driven caching. This will support more than 150 Rapid Scans, however, the maximum number of supported Rapid Scans is still being determined.
- 350 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

Note: An additional CPU, 2 GB RAM, and 100 GB of free disk space will be needed for every additional binaryscanner container.

Rapid Scanning

Rapid Scanning is now available for all customers.

Black Duck's Rapid Scanning provides a way for developers to quickly determine if the versions of open source components included in a project violate corporate policies surrounding the use of open source. Using Black Duck Detect, Rapid Scanning quickly returns results as it only employs package manager scanning and does not interact with the Black Duck server database. Use Rapid Scanning when you need quick feedback and when persisting the data in Black Duck is not necessary.

Using Rapid Scanning enables you to run thousands of scans while eliminating the need to deploy additional instances of Black Duck. It provides you with actionable results (such as failing the build) that can be used without a project version or without access to Black Duck's user interface.

New jobs subsystem

The jobs subsystem has been replaced with a new implementation.

- Possible status for a job can now be:
  - Pending
  - In progress
  - Complete
  - Error
- You can filter jobs based on their schedule: periodic or on demand.
- With the new implementation, the following jobs have been added:
  - BomAggregatePurgeOrphansCheckJob. Checks to see if any BOM data is not associated with a project version and starts the necessary jobs.
  - BomVulnerabilityDataRecomputationCheckJob. Checks if BOM computations are required when certain settings change and starts the necessary jobs.
  - BomVulnerabilityDataRecomputationJob. Updates component information received from the KnowledgeBase.
  - HierarchicalVersionBomCheckJob. Checks if hierarchical BOM computations are required and starts the necessary jobs to process them
  - JobHistoryStatsJob-Calculate Daily Statistics. Calculates daily statistics based on job activity.
  - JobHistoryStatsJob-Calculate Five Minute Statistics. Calculates statistics in 5-minute intervals based on job activity.
  - JobHistoryStatsJob-Calculate Hourly Statistics. Calculates statistics in one-hour periods based on job activity.
  - JobHistoryStatsJob-Prune Job History. Prunes old records from the job history based on the retention settings.
  - KBUpdateCheckJob. Initiates updates received from the KnowledgeBase.
  - KbUpdateWorkflowJob-BDSA Vulnerability Update. Updates BDSA vulnerability information received from the KnowledgeBase.

  - KbUpdateWorkflowJob-Component Update. Updates component information received from the KnowledgeBase.
  - KbUpdateWorkflowJob-Component Version Update. Processes component version updates received from the KnowledgeBase.
  - KbUpdateWorkflowJob-License Update. Updates license information received from the KnowledgeBase.
  - KbUpdateWorkflowJob-NVD Vulnerability Update. Updates NVD vulnerability information received from the KnowledgeBase.
  - KbUpdateWorkflowJob-Summary.Issues a summary report about the most recent KnowledgeBase update.
  - LicenseTermFulfillmentCheckJob. Checks if license fulfillment processing is required and starts the necessary jobs.
  - NotificationPurgeCheckJob. Checks if there are notifications that need cleanup and starts the necessary jobs.
  - QuartzVersionBomEventCleanupJob. Cleans up BOM events based on the retention policy.
  - VersionBomComputationCheckJob. Checks if BOM computations are required and starts the necessary jobs to process them.
  - VersionBomNotificationCheckJob. Issues notifications for BOM computation results.
  - WatchdogJob. Monitors recurring jobs to ensure they are running properly and reports on or fixes issues as they are determined.
- The following jobs have been removed:
  - KbUpdateJob

Report enhancements

- A new project version report, `license_conflicts_`*`date_time`*`.csv` has been added. It lists the license conflicts for this project version. This report has the following columns:
  - Component id
  - Version id
  - Component name
  - Component version name
  - Usage
  - License ids
  - License names
  - Source/Type
  - License Term Responsibility
  - License Term Category
  - License Term Name
  - Description
  - Conflicting License Id

  - Conflicting License Name
  - Conflicting License Term Source Type
  - Conflicting License Term Responsibility
  - Conflicting License Term Category
  - Conflicting License Term Name
  - Conflicting License Term Description
- A new column, Has License Conflicts, has been added to the end of the `components_date_time.csv` project version report. This column indicates whether this component version has a license conflict.
- File names for reports now use the system timezone instead of UTC.

Ability to refresh Black Duck KnowledgeBase copyright information

Black Duck now provides the ability for you to view updated Black Duck KnowledgeBase copyright information for a component origin. If there is new or updated data, Black Duck updates the information shown while keeping any edits that you made.

New role

A new role, BOM Annotator, has been added to Black Duck. Users with this role have read-only access to a project and can add or edit comments in a BOM and update BOM custom fields.

LDAP or SAML group synchronization

if you enabled group synchronization when configuring LDAP or SAML for Black Duck, the name of this group in the external authentication system (LDAP or SSO) now appears in the **External Group Name** field on the *Group Name* page. Now, if a group names changes on the external system, you can edit it to keep the Black Duck group name in sync with the external authentication system group name.

Enforcement of required custom fields

Black Duck now provides an option so that users *must* enter values when editing objects which have required custom fields.

New filters for project search

Black Duck now provides these filters when searching for projects:

- Never Scanned. Use this filter to find all project versions that were never part of a scan.
- Not Scanned Since. Use this filter to find all project version that have not been scanned since the selected time period.

Retention period for unmapped code locations

The default retention period for unmapped code locations has changed from 365 days to 30 days.

Additional information in the Add/Edit Component dialog boxes

So that you can more easily determine the component you wish to use, the Add Component and Edit Component dialog boxes now include the component's home page URL and the number of project versions that use this component.

Policy enhancements

The following component conditions now include a "false" option:

- License Conflict with Project Version
- Unfulfilled License Terms
- Unknown Component Version

Improved C/C++ matching

In the 2021.6.0 release, BOM accuracy has been improved for customers scanning C/C++ in the Linux domain.

New match types

Two new match types have been added in the 2021.6.0 release.

- Direct Dependency Binary. Scanning identified that the binaries in use are a direct dependency.
- Transitive Dependency Binary. Scanning identified that the binaries in use are a transitive dependency.

Supported browser versions

- Safari Version 14.0.3 (15610.4.3.1.7, 15610)
- Chrome Version 90.0.4430.72 (Official Build) (x86_64)
- Firefox Version 88.0 (64-bit)
- Microsoft Edge Version 90.0.818.41 (Official build) (64-bit)

Container versions

- 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
- blackducksoftware/bdba-worker:2021.03

- blackducksoftware/rabbitmq:1.2.2

Japanese language

The 2021.4.0 version of the UI, online help, and release notes has been localized to Japanese.

API enhancements

- With the change to the jobs subsystem:
  - The `GET /jobs/{jobID}` This call gets the job details for a specific job by ID. This call will now return a 404 Not Found status code.
  - The following calls are out-of-service since Black Duck version 2020.2.0, returning a 404 Not Found status code, and will remain non-functional in Black Duck version 2021.6.0:
    - `PUT /jobs/{jobID}` This call reschedules a job.
    - `DELETE /jobs/{jobID}` This call terminates a job.

    The functionality will be replaced with a new Job Rest API implementation which will be available in a future release.
- Added new boolean field to policy view (/api/policy-rules/{policyRuleId}) expressions ("developerScanExpression") to identify rapid scan types.

Fixed Issues in 2021.6.0

The following customer-reported issues were fixed in this release:

- (Hub-21613). Fixed an issue where the scan.cli version 2019.8.x displayed a non-meaningful warning message about performance degradation due to Java version used.
- (Hub-25227, 25521). Fixed an issue where the scan's status of Scan Complete on the Scans page was misleading.
- (Hub-26108). Fixed an issue where deploying Black Duck with Alert when using a customer certificate required manual intervention with the nginx alert configuration file.
- (Hub-26924). Fixed an issue so that a user-friendly error message now appears when a SAML SSO user login fails.
- (Hub-27209). Fixed an issue where the VersionBomComputationJob failed with the following error: "Error in job execution: could not extract ResultSet; SQL [n/a]; constraint [cvss2_severity]."
- (Hub-27681). Fixed an issue whereby the BOM Engine had to be started by a root user when deployed on Kubernetes with a custom security context.
- (Hub-27894). Fixed an issue so that the reset is set to 0 in new Black Duck searches.
- (Hub-28171). Fixed an issue where the copyright search failed for one project.
- (Hub-28305). Fixed an issue where the following error was seen in the logs: Failed class com.blackducksoftware.job.integration.domain.impl.JobMaintenanceJob.
- (Hub-28347). Fixed an issue whereby a snippet adjustment resulted in a duplicate key SnippetAdjustment error.
- (Hub-28351). Fixed a performance issue when saving BOM license changes.
- (Hub-28469). Fixed an issue where custom certificates could not be configured with Docker 20.10.x.
- (Hub-28726). Fixed an issue whereby Black Duck displayed the name of the user who cloned a project as the name of the component reviewer after the project was cloned.

- (Hub-28909). Fixed an issue where an incorrect error message appeared in the Black Duck UI after a user account was locked out.
- (Hub-29071). Fixed an issue with performance when bulk editing snippets.
- (Hub-29168). Fixed an issue where if there were no matches in a scan that was mapped to a project version, then project-level file adjustments were not applied to that project version.

Black Duck SCA 2021.4.x

New and Changed Features in Version 2021.4.1

Black Duck version 2021.4.1 is a maintenance release and contains no new or changed features.

Fixed Issues in 2021.4.1

The following customer-reported issues were fixed in this release:

- (Hub-28347). Fixed an issue where bulk snippet adjustments failed with the following error: "Adjustment Failed: The server encountered an error, please check your connection and try again."
- (Hub-28807). Fixed an issue where the following error was seen in the Artifactory plugin: "Too many parameters error on /api/projects/<projectID>/versions/<projectVersionID>/components/<componentID>/versions/<componentVersionID>?offset=0&limit=100."
- (Hub-29002). Fixed an issue where filtering for unignored snippets in the Snippet Confirmation window displayed system-wide snippets.
- (Hub-29448). Fixed an issue where the LDAP user authorization failed with an IncorrectResultSizeDataAccessException error.

Announcements for Version 2021.4.0

New containers and changes to system requirements

In the 2021.6.0 release:

- A new container, blackduck-webui, will be added for improved Black Duck performance, better caching, and future scalability.
- The Rapid Scanning feature will be available to all Black Duck customers. This feature requires a new container, currently called blackduck-kb, which will manage connections to the Black Duck KnowledgeBase and cache KnowledgeBase results for short intervals.

The following will be the minimum hardware that will be needed to run a single instance of all containers. Note that memory requirements depend on the number of concurrent Rapid Scans you want to support.

- 7 CPUs
- 28.5 GB RAM for the minimum Redis configuration; 31.5 GB RAM for an optimal configuration providing higher availability for Redis-driven caching. This will support up to 100 concurrent Rapid Scans.

  30 GB RAM for the minimum Redis configuration; 33 GB RAM for an optimal configuration providing higher availability for Redis-driven caching. This will support more than 150 Rapid Scans, however, the maximum number of supported Rapid Scans is still being determined.
- 250 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

The following is the minimum hardware that is needed to run Black Duck with Black Duck Binary Analysis.

- 8 CPUs
- 32.5 GB RAM for the minimum Redis configuration; 35.5 GB RAM for an optimal configuration providing higher availability for Redis-driven caching. This will support up to 100 concurrent Rapid Scans.

  34 GB RAM for the minimum Redis configuration; 37 GB RAM for an optimal configuration providing higher availability for Redis-driven caching. This will support more than 150 Rapid Scans, however, the maximum number of supported Rapid Scans is still being determined.
- 350 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

Note: An additional CPU, 2 GB RAM, and 100 GB of free disk space will be needed for every additional binaryscanner container.

Retention period for unmapped code locations

In the Black Duck 2021.6.0 release, the default retention period for unmapped code locations will be changing from 365 days to 30 days.

Deprecated APIs

The following endpoint has been deprecated and will be removed in a future release:

```
GET /api/scan/{scanId}/bom-entries
```

The following endpoint will be deprecated as of April 30, 2021:

```
GET /api/components/{componentId}/versions/{componentVersionId}/origins/{originId}/
direct-dependencies
```

New job implementation in 2021.6.0 release

In the Black Duck version 2021.6.0, the jobs subsystem is being replaced with a new implementation, which will cause the following job Rest API calls not to function.

- `GET /jobs/{jobID}`

  This call gets the job details for a specific job by ID. As of the Black Duck 2021.6.0 release, this call will return a 404 Not Found status code.

The following calls are out-of-service since Black Duck version 2020.2.0, returning a 404 Not Found status code, and will remain non-functional in Black Duck version 2021.6.0.

- `PUT /jobs/{jobID}`

  This call reschedules a job.
- `DELETE /jobs/{jobID}`

  This call terminates a job.

The functionality will be replaced with a new Job Rest API implementation which will be available in a future release.

Japanese language

The 2021.2.0 version of the UI, online help, and release notes has been localized to Japanese.

New and Changed Features in Version 2021.4.0

Rapid Scanning - Limited Customer Availability feature

Black Duck's Rapid Scanning provides a way for developers to quickly determine if the versions of open source components included in a project violate corporate policies surrounding the use of open source. Using Black Duck Detect, Rapid Scanning quickly returns results as it only employs package manager scanning and does not interact with the Black Duck server database. Use Rapid Scanning when you need quick feedback and when persisting the data in Black Duck is not necessary.

Using Rapid Scanning enables you to run thousands of scans while eliminating the need to deploy additional instances of Black Duck. It provides you with actionable results (such as failing the build) that can be used without a project version or without access to Black Duck's user interface.

Note: Rapid Scanning is a limited customer access feature in the 2021.4.0 release. To use Rapid Scanning, contact your Black Duck account management team for assistance.

Duplicate BOM detection

Black Duck has added duplicate BOM detection which determines if a new package manager scan duplicates the existing BOM, and if so, stops processing the scan and denotes it as complete. For high-frequency scans that generate redundant (identical) data, Black Duck's duplicate BOM detection can provide significant performance improvements.

In Black Duck 2021.4.0, this feature only impacts package manager (dependency) scans when the set of dependencies discovered by Black Duck Detect is identical to the set from the previous scan. This capability will be extended in future releases.

Ability to configure Project Manager role

Black Duck now provides the ability for system administrators to define whether the Project Manager role can manage policy violations (override policy violations or remove overrides) or remediate security vulnerabilities for a project.

By default, users with the Project Manager role can manage policy violations and remediate security vulnerabilities: users upgrading to version 2021.4.0 will not see any changes in the Project Manager role.

Multi-license editing enhancements

When editing a license for a KnowledgeBase or custom component version, Black Duck now gives you the ability to easily create new or edit existing multi-license scenarios for the components at the root level or at the same level as the original license.

Deep license data enhancement

Black Duck now provides the ability to add file level deep licenses or remove a manually added license.

Report enhancements

- The following enhancements were made to the component project version report (`component_date_time.csv`):
  - A new column, Component origin id, has been added to the end of the report. This column provides the component origin ID value that previously could only be obtained using the API.
  - The user name, date, and time was added to each comment listed in the Comments column.

- A new column, Knowledgebase Timed Out, has been added to the end of the upgrade guidance project version report (`project_version_upgrade_guidance_`*`date_time`*`.csv`). It indicates whether or not a Black Duck KnowledgeBase timeout error occurred while fetching upgrade guidance data for a component version/origin.

Policy management enhancements

- Project and component conditions available for a policy rule have been reorganized into categories to make it easier to find and select a condition. Also, custom fields for projects and components have been separated by the type of custom field.
- A new license condition, License Expiration Date Comparison for declared or deep licenses, lets you compare a license expiration date with the release date for a project version.

Vulnerability Impact enhancement

A new vulnerability condition for policy rules, Reachable from Source, is now available enabling you to create policy rules for vulnerabilities which have been identified as reachable. Use this condition to prioritize those vulnerabilities with a different (higher) priority.

Changes to LDAP or SAML group synchronization

To reduce authentication errors, Black Duck has modified LDAP or SAML group synchronization. Now, if you enabled group synchronization when configuring LDAP or SAML for Black Duck, group names on your LDAP or SAML server and the Black Duck server must be identical. If you change the name of a group in Black Duck, you must also change the name of the group on your LDAP or SAML server to match the new name (and vice versa). If the names are not identical, then the groups may be out-of-sync and user permissions for that group will be lost.

Container enhancement

A health check was added to the Binaryscanner container.

Enhancement to the Source tab

A new filter, Code View Available, has been added to the project version **Source** tab.

Component and project search enhancement

The Find page for component and project searches now provides the ability to sort search results.

Saved search enhancement

Sorted search results are supported for saved searches letting you view the results in the interested order on the Dashboard page.

Performance improvement to the *Project Name* page

To improve performance, you now must select the policy violation icon (⦸) or override icon (ⓘ) to view policy violation information on the **Overview** tab on the *Project Name* page.

Cloning enhancements

The following enhancements were made to cloning a project version:

- The default cloning options have changed. Now, all cloning options are enabled when a project is created.

- A new option, **Version Settings**, has been added which clones these values:
  - License
  - Notes
  - Nickname
  - Release Date
  - Phase
  - Distribution
- A new Clone Version dialog box appears when you select **Clone** from the *Project Name* page. If the **Version Settings** cloning option is enabled, only the new version name appears in the dialog box.
- To eliminate confusion, the **Version to Clone** field has been removed from the Create a New Version dialog box.

License conflicts enhancement

Manual edits to a BOM, including changing the usage for a component or the license of the project version using the **License Conflicts** or **Components** tab will now trigger a recalculation of the license conflict.

Enhancements to the System Information page

The usage categories on the System Information page have been enhanced.

- In the **usage: project** section, the "Scans by project" section now lists "Top 10 scans by project."
- In the **usage: rapid scan completion** section, "Rapid Scans by User" now lists the "Top 10 rapid scans by User."
- The **usage: scan completion** section has been reformatted into tables and includes an "identical package manager" row for duplicate BOM detection. Two new tables have also been added: "Code location summary information" and "Duplicate BOM information."

These pages show six months of data or the number of months the system has data, whichever value is smaller.

A new job, CollectScanStatsJob, collects scan statistics shown on the **usage: scan completion** section on the System Information page.

Removal of installation guides

The *Installing Black Duck using Kubernetes* and the *Installing Black Duck using OpenShift* guides have been removed from the documentation set. These documents only contained links to the latest documentation. These links have been added to the Black Duck documentation page in each PDF and to the home page of the online help.

Enhancement to the *Project Name* page

The *Project Name* page has been reorganized and enhanced and now includes the last scanned date for each project version.

Enhancement to the Dashboard page

The Policy Violations value for 'None" in the Policy Violations Pie Chart on the Dashboard page previously returned either 100% (no violations) or 0% (some violations), now reflects the actual percentage for violations.

Supported browser versions

- Safari Version 14.0.3 (15610.4.3.1.7, 15610)
- Chrome Version 90.0.4430.72 (Official Build) (x86_64)
- Firefox Version 88.0 (64-bit)
- Microsoft Edge Version 90.0.818.41 (Official build) (64-bit)

Container versions

- 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
- blackducksoftware/bdba-worker:2021.03
- blackducksoftware/rabbitmq:1.2.2

Japanese language

The 2021.2.0 version of the UI, online help, and release notes has been localized to Japanese.

API enhancements

- Added the capability to generate Postman collections in the API documentation through `/api-doc/postman-collection-public.json`. Users can import the `postman-collection-public.json` file as a Postman collection into Postman.
- Added the capability to generate OpenAPI Specification (OAS) for customer-facing endpoints through `/api-doc/openapi3-public.json`.
- Added the capability to filter projects by project owner by using `/api/projects?filter=owner`, which takes the URL of the user to search for the user-owned projects, for example, `/api/projects?filter=owner:https://<bd_server>/api/users/`.
- Added license ownership information as a new ownership field to the `/projects/{projectId}/versions/{projectVersionId}/components` endpoint.
- Added APIs for reading and altering the following application settings:
  - Reading analysis settings

    `GET /api/settings/analysis`

  - Updating analysis settings

    `PUT /api/settings/analysis`
  - Reading branding settings

    `GET /api/settings/branding`
  - Updating branding settings

    `PUT /api/settings/branding`
  - Reading license review settings

    `GET /api/settings/license-review`
  - Updating license review settings

    `PUT /api/settings/license-review`
  - Reading role settings

    `GET /api/settings/role`
  - Updating role settings

    `PUT /api/settings/role`
- Added `/api/component-migrations` and `/api/component-migrations/{componentOrVersionId}` endpoints to get component migration data based on specific dates or specific components from the KnowledgeBase.
- Made the `/license-dashboard` API public, which allows a user to see the in-use licenses.
- Resolved an issue with the `api/vulnerabilities/{vulnerabilityId}` endpoint returning a header overflow error when the vulnerability had over 100 references. The endpoint now provides a warning and includes meta links in the response body when 25 or more link headers are returned in the response headers.
- Removed the "Trigger type" filter from the Activity/Journal endpoints as it is only used for the "user" type.

Fixed Issues in 2021.4.0

The following customer-reported issues were fixed in this release:

- (Hub-24015, 26281). Fixed an intermittent permission denied error seen in the Black Duck user interface.
- (HUB-25116). Fixed an issue where red dots appeared in the Snippet View dialog box for a file encoded in UCS-2, rendering the text unreadable.
- (HUB-25549). Fixed an issue with `/api/uploads` where the created code location was not mapped to the project version when codeLocationName contained Japanese characters.
- (HUB-25550). Added BOM update information to a project version's activity/journal.
- (HUB-25605, 27618). Fixed an issue when using `/api/tokens/authenticate` to authenticate with an API token, where after the token expired, the HTTP client got redirected to the SAML provider page or an error occurred when generating PDF reports.
- (Hub-25993). Fixed an issue where a duplicate record caused the following error message to appear in the job runner log: 'A conflicting object already exists.'
- (Hub-26481). Fixed an issue where a page would refresh completely after saving a new remediation status.

- (HUB-26588). Fixed an issue where running a binary scan on android-studio-ide-201.7199119-windows.exe failed.
- (Hub-26695). Fixed an issue where scans took significantly longer during certain times of the day.
- (Hub-26897). Fixed an issue so that a 404 Not Found error code appears for invalid versions which are those not listed on the *Component Name* page.
- (Hub-26911). Fixed an issue where selecting an alternate snippet match incorrectly identified a component as having cryptography.
- (Hub-27159). Fixed an issue for policy rules using the 'Contributors in the past year', 'Commits in the past year' or 'New Version Count' component conditions. Although these conditions were defined to trigger a violation if the value was equal to 0, policy violations were triggered when the value was greater than 0 or a component had no commit history.

  Note: With this fix, new scans or rescans may remove some policy violations that were previously triggered.
- (Hub-27167). Fixed an issue whereby active users assigned to an inactive group with the Global Project Viewer role could see all projects in the Dashboard.
- (Hub-27175). Fixed an issue where the **Used count** value on the *Component Name* page was inaccurate as it was based on the number of component origins, not the component versions.
- (Hub-27282). Fixed an issue where the policy violation popup in the BOM occasionally got stuck open and could not be closed unless the page was refreshed.
- (Hub-27284, 27660). Fixed an issue where some dynamically linked components with a match type of transitive dependency were missing the match information in the **Source** column in the project version BOM.
- (Hub-27287). Fixed an issue so that risk counts shown on the **Overview** tab on the *Project Name* page use component version values (as the BOM page does), instead of by component origin.
- (Hub-27293). Fixed an issue where components marked as Reviewed were noted as Unreviewed when the project was rescanned.
- (Hub-27306). Fixed an issue where components were listed in case sensitive order in the Notices Report.
- (Hub-27308). Fixed an issue where the Black Duck KB *Component Name* page did not correctly show the number of vulnerabilities after the license for a component version was changed.
- (Hub-27326). Fixed an issue whereby deleting the application ID using the project's **Settings** tab did not actually delete the application ID.
- (Hub-27613). Fixed an issue where the source files for binaries could not be navigated in the **Source** tab.
- (Hub-27961). Fixed the legends for the graphs on the Dashboard page so that they did not appear clickable.
- (Hub-27982). Fixed an issue where the binary scan only identified the first and last files in an MSI archive.
- (Hub-27985). Fixed an issue with the message that appears when Black Duck is building the BOM which would disappear when you scrolled down the BOM page.
- (Hub-28094). Fixed an issue where the `/api/usergroups` endpoint was not properly using "_" or "%" in the search term.
- (Hub-28165). Fixed an issue with editing a license on the BOM page where selecting Cancel/Close still applied the changes.

- (Hub-28208). Fixed an issue where the code base size shown on the Registration page was incorrect.
- (Hub-28226). Fixed an issue so that components that are in violation of one or more policies will now generate a "policy cleared" notification when the code location that brought them in is unmapped or deleted.
- (Hub-28259). Fixed an issue with an unreview/unignore SQL query analysis.
- (Hub-28292). Fixed an issue where the HELM t-shirt sizing `.yml` files did not scale the BOM engine container.
- (Hub-28370). Fixed an issue where critical vulnerabilities were not shown when using the comparison view of the BOM.
- (Hub-28375). Fixed an issue so that the **Affected Projects** tab for a CVE or BDBA record no longer displays vulnerabilities from components that have been ignored.
- (Hub-28383). Fixed an issue where if the *Project Name* page was filtered and as a result only one version appeared on the page, the version could not be deleted.
- (Hub-28416). Fixed an issue where the AND or OR operator for a group of licenses could not be modified.
- (Hub-28458). Fixed an issue where the SnippetScanAutoBom job displayed an "Error in job execution: Duplicate key" error message.
- (Hub-28562). Fixed an issue with a binary scan where the scan failed to complete post work and the following error message appeared: "Path is not a parent of null."
- (Hub-28580). Fixed an issue when attempting to access the **My Access Tokens** page caused the following error "The application has encountered an unknown error."
- (Hub-28639). Fixed an issue where the suffix of the downloaded report file had a `.json` extension instead of `.zip` if the project name contained both English and Chinese characters.
- (Hub-28681). Fixed an issue so that the usage is shown on the **Source** tab when the match type is direct or transitive dependency.
- (Hub-28765). Fixed an issue where the BOM page displayed snippets that were both confirmed and ignored.
- (Hub-28773). Fixed an issue so that TLSv1.1 was removed from the TLS_PROTOCOLS option in the `hub-webserver.env` file.

Black Duck SCA 2021.2.x

New and Changed Features in Version 2021.2.1

Black Duck version 2021.2.1 is a maintenance release and contains no new or changed features.

Fixed Issues in 2021.2.1

The following customer-reported issues were fixed in this release:

- (Hub-23928). Fixed an issue where a confirmed snippet match was changed after a rescan.
- (Hub-26898). Fixed an issue whereby a scan appeared to be completed, however, Black Duck Detect timed out as it failed to get a bom_complete notification from Black Duck.
- (Hub-27688). Fixed an issue whereby the API call for matched files returned no information for transitive and direct dependency matches.

- (Hub-28410). Fixed an issue where the RabbitMQ container could not be started on Kubernetes which was resolved by introducing a persistent volume.
- (Hub-28208, 28386). Fixed an issue whereby the incorrect code base size was displayed on the Product Registration page.
- (Hub-28278). Fixed an issue where a missing persistent volume for RabbitMQ container caused excessive logging in the BOM Engine and scan failures.
- (Hub-28292). Fixed an issue with scaling the BOM Engine container.

Announcements for Version 2021.2.0

Notice for Azure customers

Black Duck version 2021.2.0 is being released with a known issue which impacts customers who deploy on Azure Kubernetes Services (AKS) and use Azure Database for PostgreSQL as an external database. Please note, this is the standard, recommended configuration for Black Duck customers on the Azure platform. At this time, it is NOT recommended that customers running on the Azure platform with an external database upgrade to 2021.2.0. Doing so will leave your system inoperable and force you to restore your installation back to the prior state.

We expect this to be resolved in a future release of Black Duck and will make the announcement when the release details are known.

If you are running on AKS and use an internal PostgreSQL database, there is no issue and the system works as expected. However, this would be an atypical installation on the AKS platform.

If you have concerns and questions, please reach out to Black Duck support for assistance.

Deprecation of PostgreSQL version 9.6 for external databases

Black Duck will be ending support for PostgreSQL version 9.6 for external databases starting with the Black Duck 2021.6.0 release.

As of the Black Duck 2021.6.0 release, Black Duck will only support PostgreSQL version 11.x for external databases.

Internet Explorer 11 no longer supported

Black Duck has ended support for Internet Explorer 11.

Deprecated page

The Scans > Components page is deprecated as of the 2021.2.0 release and will be removed in a future release.

Japanese language

The 2020.12.0 version of the UI, online help, and release notes has been localized to Japanese.

New and Changed Features in Version 2021.2.0

New custom vulnerability dashboards

So that you can easily view the vulnerabilities that are important to you, in 2021.2.0, the Security Dashboard has been replaced with custom vulnerability dashboards based on your saved vulnerability searches. Black Duck now provides the ability for you to search for vulnerabilities used in your projects and/or Black Duck

KnowledgeBase using a variety of attributes, save the search, and then use the Dashboard page to view dashboards from those saved searches.

For each vulnerability, the custom vulnerability dashboard displays the following information:

- BDSA or NVD vulnerability ID. Selecting the vulnerability ID shows more information on the vulnerability, such as additional score values.
- Number of project versions affected by this vulnerability with a link to view the **Affected Projects** tab for the vulnerability which lists the project versions affected by this vulnerability.
- Overall risk score.
- Whether a solution, workaround, or exploit is available.
- Date when a vulnerability was first detected, published, and last modified.
- Common Weakness Enumeration (CWE) number for this security vulnerability.

Vulnerability search enhancements

Searching for vulnerabilities has been enhanced by the attributes you can use to search for the vulnerability and the information shown in the search results. You can select whether to search for vulnerabilities in your projects or vulnerabilities in Black Duck KnowledgeBase.

The following attributes are available when searching for vulnerabilities:

- Affecting projects
- Default Remediation
- Reachable
- Exploit
- First Detected
- Remediation Status
- Solution
- Base Score
- Exploitability Score
- Impact Score
- Overall Score
- Published Year
- Severity
- Source (BDSA or NVD)
- Temporal Score
- Workaround

These vulnerability search results can now be saved and view in the Dashboard page, as described previously.

Ability to manage license conflicts for projects

To reduce the risk of license infringement, you need to understand when a component in your BOM has a license with terms that are incompatible with the declared license of a project. Black Duck now identifies these license term conflicts and displays them on a new **License Conflict** tab located on the **Legal** tab.

You can also set a policy rule that is triggered when a component's license is in conflict with the license of a project version.

Note that Black Duck only determines license conflicts for component versions with high license risk. For the Black Duck license risk model, "high risk" means that licenses in this family tend to have license conflicts under this business scenario (combination of distribution type and component usage) making them incompatible. Medium or low risks means it may have risks if the business scenario changes (or is defined incorrectly) or due to other, non-license conflicts factors.

Dependencies

When direct or transitive dependencies are found in a Black Duck Detect scan, Black Duck now lists the number of matches for each type of dependency in the project version's **Security** tab.

For transitive dependencies, a dependency tree shows the components that brought in this dependency, the vulnerabilities by severity level, and a match count for the number of times the component was brought in with that dependency path.

Report database enhancements

A new table for ignored components, (`component_ignored`, has been added to the report database. It has these columns:

- `id`. ID
- `project_version_id`. Project version ID.
- `component_id`. Component ID.
- `component_version_id`. Component version ID.
- `component_name`. Component name.
- `component_version_name`. Component version name.
- `version_origin_id`. Version origin ID.
- `origin_id`. Origin ID.
- `origin_name`. Origin name.
- `ignored`. Boolean that indicates whether the component is ignored.
- `policy_approval_status`. Policy approval status.
- `review_status`. Review status of the component.
- `reviewed_by`. User who reviewed the component.
- `reviewed_on`. When the component was reviewed.
- `security_critical_count`. Number of critical security vulnerabilities.
- `security_high_count`. Number of high security vulnerabilities.
- `security_medium_count`. Number of medium security vulnerabilities.
- `security_low_count`. Number of low security vulnerabilities.
- `security_ok_count`. Number of no security vulnerabilities.
- `license_high_count`. Number of high license risk.
- `license_medium_count`. Number of medium license risk.
- `license_low_count`. Number of low license risk.

- `license_ok_count`. Number of no license risk.
- `operational_high_count`. Number of high operational risk.
- `operational_medium_count`. Number of medium operational risk.
- `operational_low_count`. Number of low operational risk.
- `operational_ok_count`. Number of ok operational risk.

A new table for user information, `user`, has been added to the report database. It has these columns.

- `id`. ID.
- `first_name`. User's first name.
- `last_name`. User's last name.
- `username`. User's username in Black Duck.
- `email`. User's email address.
- `active`. A boolean that indicates whether this user is active.
- `last_login`. Time that the user last logged in to Black Duck.

License editing enhancements

The following enhancements were made when editing licenses in the BOM.

- When editing a license for a component, Black Duck now gives you the ability to easily create new or edit existing multi-license scenarios for the components in your BOM at the root level or at the same level as the original license.
- If you selected a different license for a component, you can now revert the license to its original license as defined in Black Duck KnowledgeBase.
- A new option in the *Component Name Version* Component License dialog box makes it easily discernible that there is an edit mode.

Report enhancement

A new column, Archive Context and Path, has been added to the end of the `source_`*`date_time`*`.csv` project version report. This column concatenates the information shown in the existing Path and Archive Content columns to provide the full path for each component.

Notices File Report

The Notices File Report has been improved so that copyright data no longer contains duplicate information for a single component-origin.

Binary scan enhancement

Binary scans now return partial matches in addition to full matches.

Deep license data enhancement

When reviewing evidence of deep license data in a file, Black Duck now highlights the license text that triggered the license text match.

BOM Engine

To improve Black Duck UI response time, license updates will now be performed by the BOM Engine. This process can be seen as a "License Update" or "License Term Fulfillment Update" event in the BOM Processing Status dialog box, accessible from the BOM.

Black Duck tutorials

To easily view training for Black Duck, you can now select **Black Duck Tutorials** from the Help menu () in the Black Duck UI.

Modification to password configuration

Users with the System Administrator role can now set password requirements for local Black Duck accounts. Users with the Super User role can no longer configure password requirements.

Policy rule enhancement

Policy management now provides the ability to create policy rules based on project version custom fields for Boolean, Date, Drop Down, Multiple Selections, Single Selection, and Text field types.

Hosting location for Black Duck Detect

Black Duck customers with limited external connectivity can now define the internal hosting location of Black Duck Detect. Using this information, these users can leverage Code Sight for deployment across their developer base to run on-demand Software Composition Analysis (SCA) scans.

Saved search dashboard enhancements

For each saved search shown on the Dashboard page, Black Duck now lists the date and time the search was last updated. A popup displays the saved search filters with a link so that you can open the Find page to edit and save a revised saved search.

Snippet triage enhancement

Icons have been added to the **Source** tab to make it easier to differentiate unconfirmed (), confirmed (), and ignored () snippets.

Supported browser versions

- Safari Version Version 14.0.3 (15610.4.3.1.6, 15610)
- Chrome Version Version 88.0.4324.150 (Official Build) (x86_64)
- Firefox Version 85.0.2 (64-bit)
- Microsoft Edge Version 88.0.705.63 (Official build) (64-bit)

Container versions

- 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
- blackducksoftware/bdba-worker:2020.12-1
- blackducksoftware/rabbitmq:1.2.2

Supported Docker versions

Black Duck installation supports Docker versions 18.09.x, 19.03.x, and 20.10.x (CE or EE).

Docker webapp-volume

The Docker webapp-volume is no longer used in orchestration. Optionally, users can backup and prune the Docker webapp-volume; otherwise no action is required.

Ubuntu operating system

The preferred operating system for installing Black Duck in a Docker environment for Ubuntu is now version 18.04.x.

Japanese language

The 2020.12.0 version of the UI, online help, and release notes has been localized to Japanese.

API enhancements

- API documentation is now only available at https://<Black Duck server URL>/api-doc/public.html.
- Added the capability to filter code locations (/api/codelocations) by creation date.
- Fixed the API used to download the SAML Identity Provider Metadata XML file (api/sso/idp-metadata endpoint) that was working incorrectly in previous versions.
- The remediation-guidance endpoint (GET /api/components/{componentId}/versions/{componentVersionId}/remediating) no longer returns a “410 GONE” response. You must switch to the upgrade-guidance endpoint, (GET /api/components/{componentId}/versions/{componentVersionId}/upgrade-guidance) which is incompatible with the remediation-guidance endpoint that was removed.
- Added a report dependency-paths endpoint to show dependency paths for a component:

  /api/project/{projectId}/version/{projectVersionId}/origin/{originId}/dependency-paths
- Added the Black Duck Detect URI endpoint which is only used to set or update reading the Black Duck Detect URI on the System Settings page:

  /external-config/detect-uri

Fixed Issues in 2021.2.0

The following customer-reported issues were fixed in this release:

- (Hub-22103). Fixed an issue whereby the Black Duck server did not respond in time when updating a license status.
- (Hub-22623). Fixed an issue whereby the Summary Dashboard frequently timed out for enterprise customers when loading in the UI.
- (Hub-24332). Fixed an issue where scanning the same code location caused duplicated notifications.
- (Hub-25374). Fixed a permission error for database azure_maintenance.
- (Hub-25580). Fixed an issue whereby components shown in the BOM were incorrectly sorted after page 9.
- (Hub-25666). Fixed a pagination issue for the endpoint /usergroups/<group #>/roles.
- (Hub-26030). Fixed an issue where sorting options were not retained for a dashboard by project name after performing an action.
- (Hub-26324). Fixed an issue where the following error "java.lang.IllegalStateException: Parent of [file:/C:/src/External/PackageManager/ProjectTemplates/com.unity.template.universal-10.1.0.tgz] does not exist" occurred when uploading a scan.
- (Hub-26343). Fixed an issue where Black Duck could not be registered as the registration container ran out of heap space.
- (Hub-26493). Fixed a confusing error message which appeared when a user removed themselves as a member of a project.
- (Hub-26501). Fixed an issue whereby the cordova-plugin-inappbrowser component could not be selected in the Edit Component dialog box.
- (Hub-26536). Fixed an issue whereby a watched project displayed the Unwatched icon () in the page header.
- (Hub-26540). Fixed an issue whereby the initial configuration of SAML did not go into effect unless Black Duck was restarted.
- (Hub-26615). Fixed an issue whereby a user with the Project Manager role in Project A and Project Manager and Project Code Scanner roles in Project B could upload scans to Project A.
- (Hub-26616). Fixed an issue whereby attempting to ignore a snippet would fail with the following error message: "Unable to update existing snippet adjustment because changing the consumer, producer, adjustment type, start line, end line is not supported."
- (Hub-26712, 26962). Fixed an issue whereby the snippet icon shown in the tree view on the **Source** tab did not clear after a snippet match was confirmed.
- (Hub-26726). Fixed an issue whereby the "not in" option was not available for custom fields when creating a policy rule.
- (Hub-26807). Fixed an issue whereby a HTML status code 404 was received when attempting to GET custom fields for the BOM component version.
- (Hub-26815). Fixed an issue whereby saving SAML integration settings caused the page to reload and switch Identity Provider Metadata settings.
- (Hub-26904). Fixed an issue whereby the match count value shown on the project version **Activity** section on the **Settings** tab was not the same as on the *Scan Name* page.

- (Hub-26930). Fixed an issue where notifications where not triggered for a component.
- (Hub-27002). Fixed an issue whereby the wrong notification was sent when a cloned project was created.
- (Hub-27049). Fixed an issue whereby the License Terms category for a Project Version Report could not be seen in the Black Duck UI without a user being assigned the License Manager role.
- (Hub-27208). Fixed an issue with blackduck-nginx whereby Black Duck Alert failed to load when SAML was configured.
- (Hub-27227). Fixed an issue whereby snippet matching took a long time to complete.
- (Hub-27264). Fixed an issue whereby reviewing a component reset its usage to its default value.
- (Hub-27681). Fixed an issue whereby the BOM Engine had to be started by a root user when deployed on Kubernetes with a custom security context.

Black Duck SCA 2020.12.x

Announcements for Version 2020.12.0

New containers and changes to system requirements

There are two additional containers: BOM Engine and RabbitMQ (now a required container) for the 2020.12.0 release.

The minimum system requirements to run a single instance of all containers are:

- 6 CPUs
- 26 GB RAM for the minimum Redis configuration; 29 GB RAM for an optimal configuration providing higher availability for Redis-driven caching
- 250 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

The minimum hardware that is needed to run Black Duck with Black Duck Binary Analysis are:

- 7 CPUs
- 30 GB RAM for the minimum Redis configuration; 33 GB RAM for an optimal configuration providing higher availability for Redis-driven caching
- 350 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

Note: An additional CPU, 2 GB RAM, and 100 GB of free disk space will be needed for every additional binaryscanner container.

Ending support for Internet Explorer 11

Support for Internet Explorer 11 is deprecated and Black Duck will be ending support for Internet Explorer 11 starting with the Black Duck 2021.2.0 release.

Japanese language

The 2020.10.0 version of the UI, online help, and release notes has been localized to Japanese.

New and Changed Features in Version 2020.12.0

New containers and changes to system requirements

There are two additional containers: BOM Engine and RabbitMQ (now a required container) for the 2020.12.0 release.

The minimum system requirements to run a single instance of all containers are:

- 6 CPUs
- 26 GB RAM for the minimum Redis configuration; 29 GB RAM for an optimal configuration providing higher availability for Redis-driven caching
- 250 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

The minimum hardware that is needed to run Black Duck with Black Duck Binary Analysis are:

- 7 CPUs
- 30 GB RAM for the minimum Redis configuration; 33 GB RAM for an optimal configuration providing higher availability for Redis-driven caching
- 350 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

Note: An additional CPU, 2 GB RAM, and 100 GB of free disk space will be needed for every additional binaryscanner container.

Password configuration

Users with the Super User role can now set password requirements for *local* Black Duck accounts. If enabled, Black Duck ensures that the new password meets your requirements and also rejects passwords that are considered weak, such as "password", "blackduck", or a user's username or email address.

Super Users can:

- define the minimum password length.
- define the minimum number of character types for the password. Possible character types are lowercase letters, uppercase letters, numbers, or special characters.
- select whether to enforce the password requirements on current users when they log in to Black Duck.

By default, *password requirements are enabled* and have these settings:

- The minimum password length is eight characters.
- Only one character type is required.
- Password requirements are not enforced on current users when logging in to Black Duck.

License enhancements

So that you can successfully manage license risk, Black Duck now gives you the ability to create new or edit existing multi-license scenarios for the components in your BOM.

Vulnerability Impact Analysis enhancements

- A new project version report, `vulnerability_matches_date_time.csv`, has been added. It lists the component, vulnerability data, and vulnerability impact analysis data for each component potentially reached by a vulnerability. This report has the following columns:
  - Component name
  - Component id
  - In use
  - Component version name
  - Version id
  - Channel version origin
  - Origin id
  - Origin name id
  - Vulnerability Id
  - Vulnerability source
  - CVSS Version
  - Security Risk
  - Base score
  - Overall score
  - Solution available
  - Workaround available
  - Exploit available
  - Called Function
  - Qualified Name
  - Line Number
- A new table, vulnerability method matches (`vulnerability_method_matches`), has been added to the report database. It has the following columns:
  - `id`. ID.
  - `project_version_id`. UUID of the project version where the reachable vulnerability appears.
  - `vuln_source`. Source of the vulnerability. For vulnerability impact analysis, the value is BDSA.
  - `vuln_id`. Vulnerability ID, such as BDSA-2020-1234.
  - `qualified_name`. Name of the class the function is called on.
  - `called_function`. Name of the vulnerable function call in your code that makes the vulnerability reachable.
  - `line_number`. Line number in your code where the vulnerable function is called.
- The vulnerability reports (vulnerability remediation report, vulnerability status report, and the vulnerability update report) now have a new column, "Reachable", added to the end of the report, to denote whether the security vulnerability is reachable (true) or not reachable (false).

BOM computation information

Black Duck now provides detailed information on the status of the computation of the project version BOM.

The new **Status** indicator (replacing the Components indicator) in the project version header in the Black Duck UI provides the current status of the BOM and notifies you of the state of the processing of BOM events. For more information, a new BOM Processing Status dialog box lists the events that are pending, processing, or have failed.

Black Duck also provides the ability to configure the frequency of the BOM event cleanup job (VersionBomEventCleanupJob) which clears those BOM events that might be stuck because of processing errors or topology changes.

Policy enhancements

- Policy management now provides the ability to create policy rules based on these custom fields:
  - Component custom fields for Boolean, Date, Drop Down, Multiple Selections, Single Selection, and Text field types.
  - Component version custom fields for Boolean, Date, Drop Down, Multiple Selections, Single Selection, and Text field types.
- You can now distinguish between declared and deep (embedded) license data when creating policy rules for these conditions:
  - License
  - License expiration date
  - License family

  Note:
  Any existing policy rules using these license conditions will now only apply to declared licenses. You must create a separate policy rule for deep (embedded) licenses for these license conditions.

Report enhancements

The vulnerability reports (vulnerability remediation report, vulnerability status report, and the vulnerability update report) that were previously only available at the global or project level are now available for project versions.

Configuration of snippet file size

You can now modify the default maximum file size that will be scanned for snippets and select a value from 1MB to 16MB.

Configuration of the clean up of unmapped code locations

Black Duck purges unmapped code location data every 365 days. You can disable this feature, such that unmapped code location data is not purged, or set the retention period to a lower number of days if you scan regularly and want to discard the data frequently.

Access tokens

The options for the scope of user access tokens are now Read or Read and Write.

Supported browser versions

- Safari Version 14.0.1 (14610.2.11.51.10)
- Chrome Version 87.0.4280.88 (Official Build) (x86_64)
- Firefox 83.0 (64-bit)
- Internet Explorer 11 11.630.19041.0

  Note that support for Internet Explorer 11 is deprecated and Black Duck will be ending support for Internet Explorer 11 starting with the Black Duck 2021.2.0 release.
- Microsoft Edge 87.0.664.60 (Official build) (64-bit)

Container versions

- 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
- blackducksoftware/bdba-worker:2020.09-1
- blackducksoftware/rabbitmq:1.2.2

Japanese language

The 2020.10.0 version of the UI, online help, and release notes has been localized to Japanese.

API enhancements

- Added ability to sort projects (api/projects) by the createdAt field.
- Added the ability to filter to the api/projects endpoint for projects created before/after a date.
- Added the API for displaying vulnerability matches as part of the Vulnerability Impact Analysis feature.

  GET /api/projects/{projectId}/versions/{projectVersionId}/vulnerabilities/{vulnerabilityId}/vulnerability-matches
- Added the following BOM endpoints:
  - Get BOM status summary:

    GET /api/projects/{projectId}/versions/{projectVersionId}/bom-status

    - List a BOM's events:

      GET /api/projects/{projectId}/versions/{projectVersionId}/bom-events
    - Delete a failed BOM event:

      DELETE /api/projects/{projectId}/versions/{projectVersionId}/bom-events/{bomEventId}
    - Delete all failed events from a BOM:

      DELETE /api/projects/{projectId}/versions/{projectVersionId}/bom-events
- New password settings endpoints:
    - Get password settings:

      GET /api/password/security/settings
    - Get system password settings:

      GET /api/password/management/settings
    - Update system password settings:

      PUT /api/password/management/settings
    - Validate password:

      POST /api/password/security/validate
- The /api/catalog-risk-profile-dashboard API now returns HTTP 404 (Not Found).

Fixed Issues in 2020.12.0

The following customer-reported issues were fixed in this release:

- (Hub-24839). Fixed an issue where some component origin IDs could not be selected from the Add/Edit Component dialog box.
- (Hub-24911). Fixed an issue where a failed KBUpdateJob skipped component updates.
- (Hub-25230). Fixed an issue where the license text window did not appear when the user attempted to open or edit license text.
- (Hub-25452). Fixed an issue so that the **Discovery Type** filter is automatically added when a license type is selected when viewing license search results page in the **Source** tab.
- (Hub-25489). Fixed an issue where the filter in the **Source** tab was reset when the subfolder was changed.
- (Hub-25603). Fixed an issue so that the path shown in the **Matched File Path** field in the Snippet View dialog box on the **Source** tab refreshed when an alternative path was selected.
- (Hub-25681). Fixed an issue where the Protex BOM Tool failed to import licenses for generic/unspecified component versions.
- (Hub-25715). Fixed an issue where the Active status in the Custom Fields Management page could not be modified unless the mouse was used.
- (Hub-25739). Fixed an issue where all comments for a BOM component could not be viewed.
- (Hub-25874). Fixed an issue where the `bom_component_custom_fields_`*`date_time`*`.csv` report listed different data than the `components_`*`date_time`*`.csv` report even though the data was in the same column name.

- (Hub-26442). Fixed an issue whereby a scan could not be deleted inside a project version by a project owner.
- (Hub-26496). Fixed an issue where a policy violation for license risk was still triggered although the license risk had changed when the component's usage was changed.

Black Duck SCA 2020.10.x

New and Changed Features in Version 2020.10.1

Container versions

- 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
- blackducksoftware/bdba-worker:2020.09-1
- blackducksoftware/rabbitmq:1.2.2

Fixed Issues in 2020.10.1

The following customer-reported issues were fixed in this release:

- (Hub-25489). Fixed an issue where the filters selected in the **Source** tab were reset when a different folder was selected.
- (Hub-25515). Fixed an issue when the host instance was running TLS 1.3 where the Signature Scanner failed when uploading and displayed the following error message: "ERROR: Unable to secure the connection to the host".
- (Hub-25791). Fixed an issue where significant increases in scan time occurred after upgrading from version 2020.4.2 to version 2020.6.1/2020.6.2.
- (Hub-26027). Fixed an issue where Black Duck displayed the following error message: "ERROR: The application has encountered an unknown error. (Bad Request) error.{core.rest.common_error" when attempting to upload a Black Duck Detect scan.
- (Hub-26085). Fixed an issue where binary scans added a second empty scan.

Announcements for Version 2020.10.0

New containers and changes to system requirements postponed to the 2020.12.0 release

Black Duck had announced previously that there would be two additional containers: BOM Engine and RabbitMQ (now a required container), for the 2020.10.0 release. This requirement has been postponed to the 2020.12.0 release.

For the 2020.12.0 release, the minimum system requirements to run a single instance of all containers will be:

- 6 CPUs
- 26 GB RAM for the minimum Redis configuration; 29 GB RAM for an optimal configuration providing higher availability for Redis-driven caching
- 250 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

For the 2020.12.0 release, the minimum hardware that is needed to run Black Duck with Black Duck Binary Analysis will be:

- 7 CPUs
- 30 GB RAM for the minimum Redis configuration; 33 GB RAM for an optimal configuration providing higher availability for Redis-driven caching
- 350 GB of free disk space for the database and other Black Duck containers
- Commensurate space for database backups

Note: An additional CPU, 2 GB RAM, and 100 GB of free disk space will be needed for every additional binaryscanner container.

Japanese language

The 2020.8.0 version of the UI, online help, and release notes has been localized to Japanese.

New and Changed Features in Version 2020.10.0

New custom component dashboards

So that you can easily view the component versions that are important to you, in 2020.10.0, the Component Dashboard has been replaced with custom component dashboards based on your saved component searches. Black Duck now provides the ability for you to search for components used in your projects using a variety of attributes, save the search, and then use the Dashboard page to view dashboards from those saved searches.

For each component version, the custom component dashboards display the following information:

- Number of project versions using this component version and for each project version, the phase, license, review status, and security risks
- Number of vulnerabilities by risk category
- License and operational risk
- Policy violations
- Approval status

- Date the component version was first detected
- Date when the component was released, according to the Black Duck KnowledgeBase
- Number of new versions
- Date when a vulnerability for the component was last updated

Component and Black Duck KnowledgeBase search enhancements

Searching for components has been enhanced by the attributes you can use to search for the component and the information shown in the search results. The UI has also been enhanced so that you can easily differentiate searches for components used in your projects and searches for components in Black Duck KnowledgeBase.

While the search attributes for Black Duck KnowledgeBase searches has not changed, the following attributes are available when searching for component versions used in your Black Duck projects:

- Security risk
- License risk
- Operational risk
- Policy rule
- Policy violation severity
- Review status
- Component approval status
- First detected
- License family
- Missing custom field data
- Release date
- License
- Vulnerability CWE
- Vulnerability reported date

For each component version matching your search criteria, the following information is shown:

- Number of project versions using this component version and for each project version, the phase, license, review status and security risks
- Number of vulnerabilities by risk category
- License and operational risk
- Policy violations
- Approval status
- Date the component version was first detected
- Date when the component was released, according to the Black Duck KnowledgeBase
- Number of new versions
- Date when a vulnerability for the component was last updated

These component search results can now be saved and view in the Dashboard page, as described previously.

For each KnowledgeBase component search result, the following information is shown:

- Number of project versions that use this component and a list of each project version, its phase, component version used, and associated security risk
- Commit activity trend
- Last commit date
- Number of component versions
- Tags for this component

Enhancement to saved searches

Black Duck now provides the ability to filter and sort saved searches on the Dashboard page.

License conflicts

In the 2020.10.0 release, Black Duck now provides the ability for you to designate incompatible custom license terms. You can define the custom license terms for forbidden or required actions that are in conflict with Black Duck KnowledgeBase terms or with your custom license terms.

Note: Currently, you cannot view incompatible license terms in a project version BOM. This ability will be available in a future Black Duck release.

License Management Enhancements

These three new filters have been added to the **License Terms** tab in License Management:

- Is Associated with License(s)
- Has Incompatible Term(s)
- Responsibility

New component usage

Black Duck has added an "Unspecified" usage which you can use to indicate that you need to investigate the usage of the component. You may find it useful to use this usage as the default value instead of existing defaults such as Dynamically Linked to eliminate confusion about whether the component is assigned its true usage value or the default value.

New tier

Black Duck has added a tier 0, which you can use to designate as the most critical tier.

Due to this new tier, these default policy rules have been modified to include tier 0:

- No External Tier 0, Tier 1 or Tier 2 Projects With More Than 1 High Vulnerability
- No External Tier 0, Tier 1 or Tier 2 Projects With More Than 3 Medium Vulnerabilities

There is no change to the existing tiers.

Enhancements to custom fields

The following enhancements have been made to custom fields

- Black Duck now provides the ability for you to denote that a custom field is required.

  - A warning message "* Additional fields are required" appears when viewing custom field information. However, users can still view and save non-custom field information and information for non-required custom fields on the page if data is not entered for the required custom field.
  - A new filter, "Missing Custom Field Data", has been added to the BOM so that you can view those components in the project version BOM which are missing information.
- An option to clear the selection has been added when viewing custom field information for Boolean and single select field types.

Allowed signature lists

Signature lists define the signatures Black Duck sends to Black Duck KnowledgeBase web service to identify the open source software contained in the your scanned code. Signature Scanner now has two new parameters which you can use to create allowed signature lists for binary or source file extensions. Each list is optional and works independently of the other list.

- **--BinaryAllowedList** *x, y, x* where *x*, *y*, *z* are the approved file extensions for SHA-1 (binary) files.
- **--SourceAllowedList** *a, b, c* where *a*, *b*, *c*, are the approved file extensions for clean SHA-1 (source code) files.

Enhancements to vulnerability impact analysis

The following enhancements have been made to vulnerability impact analysis:

- A new column, "Reachable", has been added to the end of the `security_*date_time*.csv` project version report to denote whether the security vulnerability is reachable (true) or not reachable (false).
- A new filter, "Reachable", has been added to the project version **Security** tab.

Report enhancements

The following reports have been enhanced:

- A new column, "Comments", has been added to the end of the `components_*date_time*.csv` project version report and lists the comments for each component.
- A new column, "Match type", has been added to the end of the `vulnerability-status-report_*date_time*.csv` report to identify the match type.

Enhancements to the Report Database

The following columns have been added to the component matches table (`component_matches`):

- `match_confidence`. Represents the confidence in the match, excluding snippet, binary, or partial file matches.
- `match_archive_context`. Local path to the archived file relative to the project's root directory.
- `snippet_confirmation_status`. Review status of the snippet matches.

HTTP/2 and TLS 1.3

To improve security and rendering of the Black Duck UI in a browser, Black Duck now supports HTTP/2 and TLS 1.3 in the Black Duck NGINX webserver. Note that the Black Duck NGINX Webserver continues to support HTTP/1.1 and TLS 1.2.

Change to jobs for purging scans

The BomVulnerabilityNotificationJob and the LicenseTermFulfillmentJob now also remove old audit events.

Supported browser versions

- Safari Version 13.1.2 (14609.3.5.1.5)
- Chrome Version 86.0.4240.80
- Firefox 82 (64-bit)
- Internet Explorer 11.572.19041.0

  Note that support for Internet Explorer 11 is deprecated and Black Duck will be ending support for Internet Explorer 11 starting with the Black Duck 2021.2.0 release.
- Microsoft Edge 86.0.622.51 (Official build) (64-bit)

Container versions

- 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
- blackducksoftware/bdba-worker:2020.09
- blackducksoftware/rabbitmq:1.2.2

Japanese language

The 2020.8.0 version of the UI, online help, and release notes has been localized to Japanese.

API enhancements

- Added an endpoint to determine the Single Sign-On (SSO) status of Black Duck.

  GET /api/sso/status
- Added endpoints for retrieving SAML/LDAP configurations (Admin use only).
  - Read SSO configuration:

    GET /api/sso/configuration
  - Download an IDP metadata file:

GET /api/sso/idp-metadata

- These SSO endpoints were also added:
  - Update SSO configuration:

    POST /api/sso/configuration
  - Upload an IDP metadata file:

    POST /api/sso/idp-metadata

- Added the following BOM hierarchical component endpoints:
  - List hierarchical root components:

    GET /api/projects/{projectId}/versions/{projectVersionId}/hierarchical-components
  - List hierarchical children components:

    GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/hierarchical-components/{hierarchicalId}/children
  - List hierarchical children component versions:

    GET/api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/hierarchical-components/{hierarchicalId}/children
- New fields were added to the notifications API for vulnerabilities to enable further classification of notifications. These notifications involve vulnerability information that has changed in a BOM and includes the following fields:
  - vulnerabilityNotificationCause

    Information about the kind of vulnerability event that occurred and triggered a notification such as a vulnerability was added or removed, changed comment, changed remediation details, changed severity of vulnerability, or the status changed.
  - eventSource

    Information about the source that generated the notification, such as a scan, Black Duck KB update, or user actions such as remediation, reprioritization, or adjustment.
- The /api/catalog-risk-profile-dashboard API now returns HTTP 410 (GONE).

Fixed Issues in 2020.10.0

The following customer-reported issues were fixed in this release:

- (Hub-20559, 22100). Fixed an issue where snippet adjustments were lost when scanning the same code location from a different root directory or when cloning a project version.
- (Hub-21421). Fixed an issue where the print functionality did not work for large projects.
- (Hub-23705, 25560). Fixed an issue where users could not delete reports that they created.
- (Hub-23709). Fixed an issue whereby the following scan.cli.sh warning message appeared when scanning: "Unable to find manifest from all manifests."
- (Hub-24330). Fixed an issue whereby an error message ("Duplicate key value violates unique constraint") appeared when importing a Protex project into Black Duck version 2019.10.3.
- (Hub-24673). Fixed an issue whereby navigating from a Dashboard page failed if there were more than 32,000 components.
- (Hub-24675). Fixed an issue whereby the root_bom_consumer_node_id was set incorrectly

- (Hub-24871). Fixed an issue with PostgreSQL database growth since release 2019.10.0.
- (Hub-24772). Fixed an issue where the default `.pdf` filename when printing a BOM was not the project name and version name.
- (Hub-24839). Fixed an issue where some component origin IDs could not be selected from the Add/Edit Component dialog box.
- (Hub-24947). Fixed an issue whereby search results when adding a project to a BOM were listed inconsistently.
- (Hub-25171). Fixed an issue whereby the vulnerability count was not updated when remediated using an API until after a rescan (PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/origins/{originId}/vulnerabilities/{vulnerabilityId}/remediation).
- (Hub-25219). Fixed an issue with creating reports through the API, wherein specifying a locale such as "locale" : "ja_JP" was ignored. Now, the locale field correctly sets the language of the generated report.
- (Hub-25234). Fixed an issue where the **Print** button to print a BOM was occasionally missing bar graph counts.
- (Hub-25240). Fixed an issue where browser or API calls for a specific vulnerability (BDSA-2020-1674) failed.
- (Hub-25241). Fixed an issue where the VersionBomComputationJob failed for scans with the following error message: "Data integrity violation (Constraint:not_null, Detail: on column source_start_lines)".
- (Hub-25244). Fixed an issue whereby manually added components were deleted from the BOM after upgrading to Black Duck release 2020.4.2.
- (Hub-25247). Fixed an issue whereby the following error message appeared in the Black Duck PostgreSQL logs: "ERROR: duplicate key value violates unique constraint "scan_component_scan_id_bdio_node_id_key".
- (Hub-25321). Fixed an issue where when scrolling the BOM page, text appeared in areas on the page where text should not appear.
- (Hub-25324). Fixed an issue where the Scan *Name* page did not word wrap.
- (Hub-25478). Fixed an issue where the security risk filter on the Security page became invisible.
- (Hub-25508). Fixed an issue where old media types (v4 and v5) did not always work for the policy rules API (GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/policy-rules).
- (Hub-25522, 25523). Fixed an issue where formatting issues appeared in the BOM print preview window in Chrome for Black Duck version 2020.8.0.
- (Hub-25548). Fixed an issue where selecting new component matches in the hierarchical view did not update component matches in the Source view.
- (Hub-25570). Fixed an issue whereby the Security Dashboard page only partially loaded.
- (Hub-25608). Fixed an issue where vulnerabilities were counted twice in the "New Vulnerabilities" and "New Remediated Vulnerabilities" categories in the Vulnerability Update report.
- (Hub-25649). Fixed an issue where the policy violation popup windows on the Dashboard page would not close.
- (Hub-25841). Fixed an issue whereby numbers entered into a custom field of type Text were converted into a date format.

3. Known Issues and Limitations

The following is a list of known issues and limitations in Black Duck:

New Known Issues and Limitations

- With the recent updates, Bitbucket Data Center (BBDC) now aligns with the workflow of other SCM providers, such as GitHub and GitLab, in terms of creating SCM projects. However, our QA team has identified a bug that users should be aware of:

  Issue: A limitation exists when two repositories with the same name are displayed on the same page in the UI. If one of these repositories is selected, both will be selected, resulting in both being scanned.

  Next Steps: This is a known bug, and we are actively working on a solution that will be included in the next release.

  Workaround: To avoid this issue, users can search for the exact project or repository they wish to scan and conduct the scan individually.

Current Known Issues and Limitations

- Simultaneously creating or updating serveral age-based policies may cause the BOM Engine container to run out of memory and restart, depending on system resources. If this occurs, contact Customer Support for assistance.
- Due to updates to the security ranking algorithm, searching for vulnerabilities on the Find → Vulnerabilities page may display results different from previous versions.
- When transitioning active project versions to LTS, additional vulnerabilities might the discovered in the LTS project if the active project included components identified through snippet scanning. In future updates, components matched via snippet scanning will no longer be carried over to LTS projects.
- Users of the Bitbucket Cloud SCM provider must use the same workspace name and workspace ID in Bitbucket in order to clone repositories from that workspace.
- When searching for CISA Known Exploited Vulnerabilities on the Find page, you must also check the Affecting Projects checkbox to get results. Checking only the CISA Known Exploited Vulnerability checkbox will not yield any search results.
- The Scan Heatmap found under Admin > Diagnostics > Heatmaps displays results in UTC time instead of local time. Please be aware of this when using this new feature.
- Components marked for deletion based on Match Score threshold setting are not being removed when re-uploading BDIO through UI.
- The **Purge ONLY Archived Project Version Unmatched Scan File Data** and **Purge All Unmatched File Data** links do not work at both the project (*project* > Settings tab) and global (Admin > System Settings > Data Retention) levels.
- If you are using an LDAP directory server to authenticate users, consider the following:
  - Black Duck supports a single LDAP server. Multiple servers are not supported.
  - If a user is removed from the directory server, Black Duck user account continues to appear as active. However, the credentials are no longer valid and cannot be used to log in.
  - If a group is removed from the directory server, Black Duck group is not removed. Delete the group manually.

- Tagging only supports letters, numbers, and the plus (+) and underscore (_) characters.
- If Black Duck is authenticating users, user names are not case sensitive during login. If LDAP user authentication is enabled, user names are case sensitive.
- If a code location has a large bill of materials, deleting a code location may fail with a user interface timeout error.