Black Duck SCA 发行说明

Black Duck SCA 2025.7.0

04-11-2025

内容

前言

Black Duck 文档

Black Duck 的文档包括在线帮助和以下文档：

标题	文件	说明
发行说明	release_notes.pdf	包含与当前版本和先前版本中的新功能和改进功能、已解决问题和已知问题有关的信息。
使用 Docker Swarm 安装 Black Duck	install_swarm.pdf	包含有关使用 Docker Swarm 安装和升级 Black Duck 的信息。
使用 Kubernetes 安装 Black Duck	install_kubernetes.pdf	包含有关使用 Kubernetes 安装和升级 Black Duck 的信息。
使用 OpenShift 安装 Black Duck	install_openshift.pdf	包含有关使用 OpenShift 安装和升级 Black Duck 的信息。
入门	getting_started.pdf	为初次使用的用户提供了有关使用 Black Duck 的信息。
扫描最佳做法	scanning_best_practices.pdf	提供扫描的最佳做法。
SDK 入门	getting_started_sdk.pdf	包含概述信息和样本使用案例。
报告数据库	report_db.pdf	包含有关使用报告数据库的信息。
用户指南	user_guide.pdf	包含有关使用 Black Duck 的 UI 的信息。

在 Kubernetes 或 OpenShift 环境中安装 Black Duck 软件的安装方法是 Helm。单击以下链接查看文档。

- Helm 是 Kubernetes 的软件包管理器，可用于安装 Black Duck。 Black Duck 支持 Helm3，Kubernetes 的最低版本为 1.13。

Black Duck 集成文档位置：

- https://sig-product-docs.blackduck.com/bundle/detect/page/integrations/integrations.html
- https://documentation.blackduck.com/category/cicd_integrations

客户支持

如果您在软件或文档方面遇到任何问题，请联系 Black Duck 客户支持：

- 在线： https://community.blackduck.com/s/contactsupport
- 要创建支持案例，请登录 Black Duck Community 网站：https://community.blackduck.com/s/contactsupport。
- 另一个可随时使用的方便资源是在线社区门户。

Black Duck 社区

Black Duck 社区是我们提供客户支持、解决方案和信息的主要在线资源。该社区允许用户快速轻松地打开支持案例，监控进度，了解重要产品信息，搜索知识库，以及从其他 Black Duck 客户那里获得见解。社区中包含的许多功能侧重于以下协作操作：

- 连接 - 打开支持案例并监控其进度，以及监控需要工程或产品管理部门协助的问题
- 学习 - 其他 Black Duck 产品用户的见解和最佳做法，使您能够从各种行业领先的公司那里汲取宝贵的经验教训。此外，客户中心还允许您轻松访问 Black Duck 的所有最新产品新闻和动态，帮助您更好地利用我们的产品和服务，最大限度地提高开源组件在您的组织中的价值。
- 解决方案 - 通过访问 Black Duck 专家和我们的知识库提供的丰富内容和产品知识，快速轻松地获得您正在寻求的答案。
- 分享 - 与 Black Duck 员工和其他客户协作并进行沟通，以众包解决方案，并分享您对产品方向的想法。

访问客户成功社区。如果您没有帐户或在访问系统时遇到问题，请单击此处开始，或发送电子邮件至 community.manager@blackduck.com。

培训

Black Duck “客户教育”是满足您所有 Black Duck 教育需求的一站式资源。它使您可以全天候访问在线培训课程和操作方法视频。

每月都会添加新视频和课程。

在 Black Duck 教育，您可以：

- 按照自己的节奏学习。
- 按照您希望的频率回顾课程。
- 进行评估以测试您的技能。
- 打印完成证书以展示您的成就。

要了解更多信息，请访问 https://blackduck.skilljar.com/page/black-duck，或者，要获取 Black Duck 的帮助信息，请选择 Black Duck 教程（从“帮助”菜单（  ）（位于 Black Duck UI 中）选择）。

Black Duck 关于包容性和多样性的声明

Black Duck 致力于打造一个包容性的环境，让每位员工、客户和合作伙伴都感到宾至如归。我们正在审查并移除产品中的排他性语言以及支持面向客户的宣传材料。我们的举措还包括通过内部计划从我们的工程和工作环境中移除偏见语言（包括嵌入我们软件和 IP 中的术语）。同时，我们正在努力确保我们的 Web 内容和软件应用程序可供不同能力的人使用。由于我们的 IP 实施了行业标准规范，目前正在审查这些规范以移除排他性语言，因此您可能仍在我们的软件或文档中找到非包容性语言的示例。

Black Duck 安全承诺

作为一家致力于保护和保障客户应用程序安全的组织，Black Duck 同样致力于客户的数据安全和隐私。本声明旨在为 Black Duck 客户和潜在客户提供关于我们的系统、合规性认证、流程和其他安全相关活动的最新信息。

本声明可在以下位置获取：安全承诺 | Black Duck

1. Black Duck SCA 2025.7.0

公告

PostgreSQL 容器即将迁移到版本 16

从 2025.10.0 版本开始，Black Duck 将把 PostgreSQL 容器映像升级到 PostgreSQL 16。此次迁移可确保性能和稳定性得到提升，并使用户可访问最新的 PostgreSQL 功能。使用打包版 PostgreSQL 容器的客户应在升级前验证其环境与 PostgreSQL 16 的兼容性。使用外部数据库的客户无需采取任何操作。

即将对 PostgreSQL 容器用户实施升级限制

从 2025.10.0 版本开始，Black Duck 将仅支持从已使用 PostgreSQL 14 或 15 的版本（具体为 Black Duck 2023.10.0 到 2025.7.x 版本）直接升级到捆绑的 PostgreSQL 容器（PostgreSQL 16）。

如果您使用的 Black Duck 版本早于 2023.10.0，则需要执行两步升级：

1. 首先升级到 2024.7.x
2. 然后升级到 2025.10.x

此更改仅适用于使用 Synopsys 提供的 PostgreSQL 容器的用户。使用外部数据库配置的用户不受影响。

即将终止对 PostgreSQL 15 的支持

对 PostgreSQL 15 的支持将在 Black Duck 的 2025.10.0 版本中结束。

当前使用 PostgreSQL 15 容器的用户应计划在该版本发布前升级到 PostgreSQL 16。

外部数据库配置应遵循标准兼容性指南。

延长对 PostgreSQL 17 支持的测试期

Black Duck 将延长 PostgreSQL 17 作为外部数据库选项的仅测试用途期限，因为 PG 17.x 被发现存在性能下降问题。尽管我们正在进行调查以解决此问题，但不建议此时在生产环境中使用 PG 17.X。因此，对 PG 17.x 的仅评估支持已延长。

请注意，此扩展不影响我们计划在 Black Duck 2025.10.0 版本发布时终止对 PostgreSQL 15.x 的支持。请关注后续更新，我们将努力在未来版本中实现对 PostgreSQL 17.x 的全面生产支持。

新要求：PostgreSQL 的 pg_trgm 扩展

从 Black Duck 2025.7.0 版本开始，bds_hub 数据库需要 pg_trgm PostgreSQL 扩展。

- 如果使用 Black Duck 提供的 PostgreSQL 容器，则无需任何操作，扩展将在升级过程中自动安装。
- 如果使用外部 PostgreSQL 实例，则升级过程将尝试安装扩展。但是，这可能在具有受限权限的环境（例如 Amazon RDS 或其他托管服务）中失败。

为避免迁移问题，Black Duck 强烈建议在升级到 2025.7.0 之前，确保在 bds_hub 数据库中安装了 pg_trgm 扩展。

- 对于托管服务，请参阅提供商的文档，以获取有关启用数据库扩展的说明。
- 对于标准的 PostgreSQL 安装，您可以使用以下命令手动安装该扩展：

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

即将合并 scan 和 matchengine 容器

在 2025.10.0 版本中，scan 和 matchengine 容器将合并为一个 scanmatch 容器。此更改是为减少资源需求并简化 Black Duck SCA 部署所做持续努力的一部分。

即将弃用扫描端点

为了提高可维护性并简化 Black Duck API，计划在即将发布的版本中弃用一些与扫描相关的旧版端点。下表列出了受影响的端点及其弃用时间表。

- 对于支持多种扫描类型的端点，只有明确列出的扫描类型会受到影响。
- 对于使用任何受影响端点的客户，建议联系客户团队或技术支持，以获取协助或迁移指导。

使用完全受支持的 Detect 版本（9、10）的客户在移除 API 时不会受到影响，无需采取任何行动。所有受支持的 Detect 版本均不依赖于计划在 2026.4.0 版本中移除的 API。到 2027.4.0 版本，Detect 11 将成为最旧的受支持版本，且不使用任何已废弃的 API。有关更多信息，请参阅 Black Duck Detect 支持和服务终止时间表。

API 端点	内容类型	弃用于	移除于	扫描类型
POST /v1/scans	NULL, application/vnd.blackducksoftware.internal-cli-1	2025.7.0	2026.4.0	• 软件包管理器 • 签名
PUT /v1/scans/{scanId}	NULL, application/vnd.blackducksoftware.internal-cli-1	2025.7.0	2026.4.0	• 软件包管理器 • 签名
POST /bom-import	application/ld+json	2025.7.0	2028.1.0	• 软件包管理器 • 签名
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	• 软件包管理器 • 签名 • 二进制 • 容器
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	2025.7.0	2027.4.0	• 软件包管理器 • 签名 • 二进制 • 容器

	application/vnd.blackducksoftware.intelligent-persistence-scan-3+protobuf			
POST /uploads	multipart/form-data	2025.1.0	2027.4.0	• 二进制
POST /uploads/multipart	application/vnd.blackducksoftware.binary-multipart-upload-start-1+json	2025.1.0	2027.4.0	• 二进制
PUT /uploads/multipart/{scanId}	application/vnd.blackducksoftware.multipart-upload-data-1+octet-stream	2025.1.0	2027.4.0	• 二进制
POST /uploads/multipart/{id}/completed	application/vnd.blackducksoftware.multipart-upload-finish-1+json	2025.1.0	2027.4.0	• 二进制
POST /storage/containers/{scanId}	application/vnd.blackducksoftware.container-scan-data-1+octet-stream	2025.1.0	2027.4.0	• 容器
POST /storage/containers/{id}/message	application/vnd.blackducksoftware.container-scan-message-1+json	2025.1.0	2027.4.0	• 容器
POST /storage/containers/{id}/multipart	application/vnd.blackducksoftware.multipart-upload-start-1+json	2025.1.0	2027.4.0	• 容器
PUT /storage/containers/{id}/multipart	application/vnd.blackducksoftware.multipart-upload-data-1+octet-stream	2025.1.0	2027.4.0	• 容器
POST /storage/containers/{id}/multipart/completed	application/vnd.blackducksoftware.multipart-upload-finish-1+json	2025.1.0	2027.4.0	• 容器

新增和更改的功能

新增对 GitHub 应用程序的集成支持

Black Duck 现在支持与新的 GitHub 应用程序集成，这是一款新的 SCM 接入应用程序，旨在简化和自动化将 GitHub 连接到 Black Duck 的过程。集成后，GitHub 应用程序会执行扫描并将结果直接发送到 Black Duck，从而简化接入，并集中查看开源风险。有关设置详细信息和配置指南，请参见 GitHub 应用程序集成指南。

使用新的“漏洞”选项卡更新项目版本 BOM 视图

项目版本 BOM 视图中的“安全”选项卡已替换为新的“漏洞”选项卡。这个重新设计的选项卡改进了布局，同时将继续提供关键的漏洞洞察。用户现在可以从增强的过滤选项、更清晰的漏洞数据展示以及对修复详情的更快捷访问中受益，而所有这些都在更直观的界面中实现。

增加对 SPDX v3.0 的支持

Black Duck 现在支持以 SPDX v3.0 格式导入和导出软件材料清单 (SBOM)。这提高了与现代工具的兼容性，并增强了对 SBOM 数据结构的支持。

有关 SPDX v3.0 规范的更多信息，请访问 SPDX v3.0 参考页面。

在 SBOM 报告中添加了对 SBOM 类型字段的支持

Black Duck SBOM 报告现在包含一个新的 SBOM 类型字段，用于标识 SBOM 所代表的软件生命周期阶段。支持的值包括 Design、Source、Build、Analyzed、Deployed 和 Runtime，符合 CISA 的 SBOM 文档指南。

此增强功能通过帮助使用者了解所提供数据的上下文和完整性，提高了 SBOM 的清晰度和可追溯性。

向 SBOM 新增对组件哈希的支持

Black Duck SBOM 现在支持新的组件哈希功能，使用户能够为组件添加加密标识符。在 SBOM 模板中启用该功能后，用户可以填充两个新字段：

- 哈希值：一个唯一的加密哈希值，用于在扫描时标识组件的内容。
- 哈希算法：用于计算哈希值的算法（例如，SHA-256）。

此增强功能提高了可追溯性，并支持跨 SBOM 的完整性验证。

停用 ReversingLabs 功能

已从 Black Duck 中完全移除对 ReversingLabs 功能的支持。这包括移除所有先前已弃用的功能、API 以及与 ReversingLabs 相关的架构引用。剩余的所有公共 ReversingLabs API 现在都将返回 410 Gone 响应，或被标记为已弃用。作为此更改的一部分，所有文档引用也已移除。

如果您使用 ReversingLabs 集成，我们建议您审查您的工作流程，并过渡到受支持的替代方案。

术语从“总体角色”更新为“全局角色”

为了在整个产品范围内提高清晰度和一致性，所有对“总体角色”的引用都已更新为“全局角色”。此更改统一了术语，能够更好地反映了这些角色在 Black Duck 中的范围和功能。仅名称发生了变化，角色职能和权限保持不变。

更新过滤器行为以包含 LTS 项目

“查找”→“漏洞”页面上的“影响项目”过滤器已更新，以包含长期支持 (LTS) 项目。启用后，此过滤器现在会将结果限制为在活动项目和 LTS 项目中发现的漏洞，使用户能够更全面地查看影响受支持版本的风险。

代码段扫描支持新的文件类型

Black Duck 现在支持对 Kotlin (.kt) 和 Rust (.rs) 文件进行代码段扫描。这些新增功能扩展了语言覆盖范围，并提高了分析过程中的代码段识别能力。无需配置更改：扫描将自动检测并处理这些文件类型。

无障碍性改进

此版本引入了多项旨在增强 Black Duck 整体无障碍性和可用性的更新。这些更改改进了对辅助技术的支持，更符合 WCAG 等无障碍性标准。

- 改进了全局搜索 → 下拉菜单的无障碍性。
- 现在可以通过键盘访问“管理”和“管理员”侧边菜单。
- 现在，下拉菜单在展开后，可以通过键盘导航，并可用 Escape 键关闭。在菜单组件关闭前，焦点将保持在组件内。
- 提高了扫描错误消息的对比度。
- 改进了 SBOM 输入字段的标签，为键盘和屏幕阅读器导航提供更好的支持。

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

弃用组件漏洞 API 端点

以下 API 端点现已标记为弃用：

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

为了提高准确性，漏洞现在可以更有效地映射到：

- 组件版本：

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

- 组件来源：

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

因此，我们建议客户过渡到使用文档中记录的端点，以应对组件版本漏洞和组件来源漏洞。未来版本将限制从已废弃端点返回的数据量，并且其后续版本将完全移除该 API。建议用户相应更新其实现，以确保可继续访问漏洞数据。

二进制扫描程序信息

二进制扫描程序已更新为版本 2025.3.1。

版本亮点和已修复的问题

-

已修复的问题

此版本中修复了以下客户报告的问题：

- （HUB-34976、HUB-39582）。修复了以下问题：扫描客户端无法解包某些 TAR 存档文件。以前，部分 TAR 文件被视为单个文件，未被正确地解包和扫描。扫描客户端现在可以正确检测和处理这些存档文件。
- (HUB-38990)。修复了以下问题：项目过滤器在扫描映射对话框中可能不会返回结果。
- (HUB-43218)。修复了以下问题：在使用 SPDX 2.3 生成的 SBOM 报告中，标签:值格式无法通过 SPDX ntia-conformance-checker 检查。
- (HUB-43300)。修复了以下问题：/api/notifications/{notifications id} 未强制执行适当的基于用户的授权。
- (HUB-43916)。修复了以下问题：SCASS 扫描未遵守代理设置。
- (HUB-43992)。修复了 null 'MatchAmbiguityDetail' 在 Black Duck 特征扫描期间导致的 NullPointerException 错误。
- (HUB-44199)。修复了以下问题：使用 PUT /api/projects/{projectId}/versions/{projectVersionId}/bulk-snippet-bom-entries 端点时，用户可能会间歇性收到“无法管理代码段调整”错误消息。
- (HUB-44217)。修复了以下问题：Black Duck 可能不会处理大于 10 MB 的 BDMU 文件。
- (HUB-44246)。为 Code Sight 客户更新了关于“Black Duck Detect 托管位置”的 Black Duck SCA文档。
- (HUB-44352)。修复了以下问题：st.iscomponentignored 函数未忽略 IGNORED_SNIPPETignore_status。
- (HUB-44469)。从系统信息调试页面移除了 dbschema 部分。

- (HUB-44497)。修复了以下问题：如果从 LTS 项目版本开始浏览，即使不存在活动版本，用户也会返回到“活动版本”选项卡。
- (HUB-44533)。修复了以下问题：在 Docker 26 版本上（使用“--detect.docker.image”）或在基于 Docker 26 版本创建的映像上（使用“detect.docker.tar”）扫描 Docker 映像时，未启用精确文件匹配。
- (HUB-44574)。修复了以下问题：通过 SCASS 执行的软件包管理器扫描未返回匹配置信度。
- (HUB-44586)。修复了以下问题：在 DAST 扫描期间，隐藏目录（/css/、/js/、/images/、/fonts/）返回 403 错误而不是 404 错误。
- (HUB-44625)。解决了以下问题：项目版本在转换为 LTS 期间卡住，导致 UI 旋转以及重新扫描因数据库冲突而失败。
- (HUB-44675)。修复了以下问题：由于数据库中出现重复键约束冲突，导致在同一代码位置进行并行扫描时出现间歇性“500 内部服务器错误”。
- (HUB-44684)。改进了生成项目版本许可证条款报告的性能。
- (HUB-44738)。修复了以下问题：在 Black Duck 中单个二进制扫描出现重复来源树。该问题与从 jsonld 格式切换到 protobuf 格式有关，已通过代码更改和清理旧扫描数据的后台作业修复。
- (HUB-44807)。修复了 Webapp 风险概况计算中的问题，该问题由于“来源”视图代码中缺少循环依赖检查而引起。该修复可阻止在项目版本之间创建直接循环引用的调整，确保正确处理错误并避免无限循环。
- (HUB-44811)。修复了以下问题：将文件夹或文件映射到组件时显示成功消息，但未在“组件”选项卡中更新组件名称。该修复在不允许编辑时禁用“编辑”按钮，并确保 UI 使用正确的 PUT API 进行调整。
- (HUB-44844)。修复了以下问题：具有“项目管理员”或“项目经理”角色的用户能够通过 GET /api/tokens 端点读取所有用户访问令牌。
- (HUB-44845)。修复了以下问题：具有项目级别“项目管理员”或“项目经理”角色的用户能够与他们没有直接/间接访问权限的项目进行 BOM 比较。
- (HUB-44888)。解决了以下问题：组件页面未指明组件是否在长期支持 (LTS) 项目中使用。这阻止了用户识别哪些 LTS 项目可能受到与该组件相关漏洞的影响。
- (HUB-44890)。解决了以下问题：“matched-files”REST API 在多个扫描中将同一组件的匹配计数错误地计算为一，导致 API 响应中 totalCount 和 items 不匹配。
- (HUB-44923)。修复了以下问题：Docker Swarm 部署完成后，Black Duck 登录屏幕上“服务器不可用”消息可能长时间持续存在。
- (HUB-44924)。修复了以下问题：任何经过身份验证的用户都可以通过 GET /api/codelocations/<code-location-id>/scan-summaries 端点查看代码位置的扫描摘要。
- (HUB-44925)。修复了以下问题：从某些 API 端点（如 /api/users、/api/risk-profile-dashboard 和 /api/codelocations）导出的 CSV 文件包含用户提供的输入，可能导致公式注入。现已正确清理用户输入，以防止此行为。此修复已应用于 Black Duck 中所有使用用户输入生成 CSV 文件的区域。
- (HUB-44958)。修复了以下问题：尝试更改组件的“使用”类型时（例如，从“前提条件”更改为“动态链接”），显示成功消息但未保存更改。该问题仅限于某些“使用”类型，而其他类型（如“源代码”）则按预期工作。
- (HUB-44971)。解决了以下问题：在分配了项目代码扫描程序角色后，用户在特征扫描期间仍遇到 403 错误。该问题与从 2024.4.1 版本升级到 2025.1.1 版本后特定数据集不一致有关，在全新的 HUB 实例上无法重现。
- (HUB-45073)。修复了以下问题：在导入期间未自动创建 SBOM 中带有 Black Duck 参考 ID 的自定义组件，导致 BOM 不完整。

- (HUB-45082)。解决了以下问题：移动项目组导致其描述被移除，显示“无描述”。该修复可确保在“管理”→“项目组”界面中移动组时保留组描述。
- (HUB-45087)。修复以下问题：scan_start_at 在 scan_view 和 scan_stats_view 中映射不正确，使用了 CL 创建时间而不是实际扫描开始时间。这导致同一 CL 上的所有扫描共享相同的开始日期。映射已更正为反映准确的扫描开始时间。
- (HUB-45100)。修复了以下问题：使用 update=true 克隆项目版本时未保留原始请求中“未知许可证”值。
- (HUB-45112)。修复了以下问题：如果“工具”字段缺失，尽管根据 CycloneDX 1.4 规范，该字段不是必需的，但 Black Duck 将无法处理有效的 CycloneDX 1.4 SBOM。该修复可确保即使没有“工具”字段，SBOM 也能成功得到处理，与模式要求保持一致。
- (HUB-45139)。修复了以下错误：BDBA protobuf BDIO 扫描中的组件无法像 JSON BDIO 扫描那样，在 HUB UI 中正确显示。该问题与匹配方法的差异及 API 不一致有关。KBAPI 6.2.0 更新解决了这些匹配问题，提高了 protobuf BDIO 组件的可见性，但仍需 HUB 端的继续修复才能彻底解决。
- (HUB-45140)。修复了以下问题：在策略规则的项目条件中添加的自定义字段显示重复值而不是正确单个条目。
- (HUB-45142)。修复了以下问题：Rocky Linux 的某些组件未在 Black Duck 扫描中显示正确来源 ID 或命名空间。
- (HUB-45167)。修复了以下问题：在 2025.1.1 版本中，当参考定位符包含空格时，会导致 SPDX 报告生成失败。
- (HUB-45186)。修复了以下问题：未履行的许可证在政策违规视图中，其许可证履行条款未能正确显示。在法律条款选项卡中所做的更改未更新版本视图，导致概览视图和 BOM 视图之间不一致。该修复确保了当许可证条款被标记为已履行时，各视图之间准确同步。
- (HUB-45187)。解决了以下问题：除非将组件版本的批准状态设置为“未审核”，否则加密数据无法显示。该问题源自未正确处理除“未审核”之外的批准状态，阻止了加密数据的正确填充。
- (HUB-45213)。修复了以下问题：对于匹配类型为“精确”和“二进制及文件已修改”的组件，版本报告中缺少匹配内容。
- (HUB-45353)。针对用于创建自定义特征的 IFM 属性，更正了文档错误。文档错误地将该属性列为 --blackduck.signature.scanner.individual.file.matching，但应该为 --detect.blackduck.signature.scanner.individual.file.matching。
- (HUB-45354)。更新了 Artifactory 插件安装文档，将过时的 sig-repo URL 替换为正确的 URL。
- (HUB-45389)。更新了自定义扫描特征的描述，使其更符合其实际功能。
- (HUB-45396)。解决了以下问题：由于 PURL 中“+”字符编码不正确，SBOM 导入导致组件出现不匹配。该编码错误将“+”转换成“%20”而不是“%2B”，从而导致查找失败。该修复确保了编码正确，使 PURL 查找和组件匹配能够成功。
- (HUB-45488)。修复了以下问题：“用户组”页面上出现角色重复。
- (HUB-45515)。修复了 ASML 遇到的特征扫描失败 (ERR05_1076)，该问题由 Hub 系统中的 NullPointerException 引起。该问题源于 MaaS 端修复后 ScanMatchNode 通道版本为空。该修复包括更新 Hub 对空 ScanMatchNode 的处理。
- (HUB-45530)。重新启用了针对所有二进制匹配的源文件调整，并恢复了 Black Duck 2024.10.0 版本中存在的功能。
- (HUB-45620)。解决了以下错误：在父项目的组件报告中，一个子项目中关于组件的评论被错误地归属于所有子项目。该修复现在确保了将评论正确地限制在它们所属的子项目中。
- (HUB-45659)。修复了以下 UI 问题：在项目、项目版本、组件等的自定义字段页面上出现“无法加载自定义字段”横幅错误。尽管出现错误，查看和编辑自定义字段的功能不受影响。

2. 之前的 Black Duck SCA 版本

Black Duck SCA 2025.4.x

Black Duck SCA 2025.4.2

公告

目前尚未发布有关 Black Duck 2025.4.2 的新公告。

新增和更改的功能

Black Duck 2025.4.2 中没有新增或更改的功能。

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

Black Duck 2025.4.2 版本中没有新的或更改的 API 请求。

二进制扫描程序信息

Black Duck 2025.4.2 中，二进制扫描程序没有新增或更改的功能。

已修复的问题

此版本中修复了以下客户报告的问题：

- (HUB-45342)。修复了以下问题：由于 version_bom_risk_status 中存在的残留数据，导致 version_bom_risk_warning 中的忽略状态标志与修复状态不一致。该问题可追溯到迁移脚本在 version_bom_risk_status 中遗留的数据，导致忽略的标志被错误地恢复。该修复通过重新运行迁移脚本，并删除状态为 REMEDIATED 但 ignored 为 false 的特定记录，确保忽略的标志与修复状态正确同步。
- (HUB-45481)。解决了以下问题：由于未优化升级脚本，升级到 2025.4.1 版本耗时过长。已优化该脚本，以显着提高升级性能。
- (HUB-45490)。解决了以下问题：KB 更新作业偶尔未能使用新识别的漏洞更新某些项目版本。在调查过程中，发现组件版本的漏洞计数在各个项目版本之间不同步。在此次更新中，已刷新受影响组件版本的 BOM，以提高准确性。然而，BOM 刷新后出现的新组件目前不会自动更新。我们正在积极开发进一步的改进，以在未来的版本中提供更全面的解决方案。
- (HUB-45609)。修复了在端点 /api/vulnerabilities/{vulnerability_id}/affected-bom-components 的查询中由参数顺序错误导致的 SQL 错误。该问题将导致 BadSqlGrammarException 和 PostgreSQL 错误，提示 ~~* 操作符与参数类型不匹配（text 与 UUID）。该修复更正了查询的参数顺序，以在所有命名空间中确保正确执行。
- (HUB-45699)。通过优化查询计划，提高了 components-in-use API 的性能，从而显著减少了执行时间和资源使用。之前的实现会导致排序期间出现过量数据处理和磁盘溢出。通过简化查询逻辑，该修复大幅减少了系统开销并提高了响应速度，使 API 更高效、更实用。

Black Duck SCA 2025.4.1

公告

目前尚未发布有关 Black Duck 2025.4.1 的新公告。

新增和更改的功能

Black Duck 2025.4.1 中没有新增或更改的功能。

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

Black Duck 2025.4.1 版本中没有新的或更改的 API 请求。

二进制扫描程序信息

Black Duck 2025.4.1 中，二进制扫描程序没有新增或更改的功能。

已修复的问题

此版本中修复了以下客户报告的问题：

- （HUB-45290、HUB-45293、HUB-45332、HUB-45360）。此版本重新解决了一个问题：漏洞修复状态被错误地应用于组件版本所有来源。原始修复包含数据库迁移和代码更改，但由于 KnowledgeBase 更新作业，修复状态可能仍不同步。此次更新更全面地修正了该问题，确保修复状态按照来源得到一致地应用。

  此外，数据库迁移脚本已更新，以防止在升级过程中子项目风险计数被重置。升级后，子项目风险可能会在项目汇总中短暂显示为缺失；这些值将在服务器重启后大约 10 分钟内由 BOM 漏洞重新计算检查自动重新计算。完成此作业后，子项目的计数将更新。存档的项目必须先取消存档，才能刷新其 BOM。如需进一步协助，请联系 Black Duck 客户支持。

  注意：此修复包含数据库迁移。对于拥有大型数据库的客户，迁移过程可能需要一小时或更长时间才能完成。

- (HUB-45300)。修复了以下问题：API 中更严格的时间戳解析导致 issueCreateAt 和 issueUpdatedAT 字段处理失败，影响通过 Alert 8.0.1 与 JIRA 等问题跟踪系统的集成。通过引入回退解析器来接受额外的时间戳格式，该问题得以解决。
- (HUB-45349)。暂时移除了组件版本页面“安全”选项卡上的漏洞计数标签。为避免混淆，在我们解决该计数标签的准确性问题期间，已将其移除。问题解决后，该标签可能会在未来的版本中恢复。

已知问题

下面列出了 Black Duck SCA 中新增的已知问题和限制：

- 在某些情况下，最初显示正确的修复状态可能会在几天后变得不同步。此问题被认为与自动化修复工作流程有关，且仅影响某些漏洞。该问题正在调查中。
- 在极少数情况下，漏洞的忽略状态可能与其修复状态不一致。具体来说，某些漏洞即使状态显示为“新增”或“需要修复”，也可能显示为已忽略。此问题主要影响较旧的漏洞，目前正在调查中。

Black Duck SCA 2025.4.0

公告

即将实施的要求：PostgreSQL 的 pg_trgm 扩展

从 Black Duck 2025.7.0 版本开始，bds_hub 数据库将需要 pg_trgm PostgreSQL 扩展。

- 如果使用 Black Duck 提供的 PostgreSQL 容器，则无需任何操作，扩展将在升级过程中自动安装。
- 如果使用外部 PostgreSQL 实例，则升级过程将尝试安装扩展。但是，这可能在具有受限权限的环境（例如 Amazon RDS 或其他托管服务）中失败。

为避免迁移问题，Black Duck 强烈建议在升级到 2025.7.0 之前，确保在 bds_hub 数据库中安装了 pg_trgm 扩展。

- 对于托管服务，请参阅提供商的文档，以获取有关启用数据库扩展的说明。
- 对于标准的 PostgreSQL 安装，您可以使用以下命令手动安装该扩展：

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

初步支持 PostgreSQL 17

Black Duck 2025.4.0 引入了对使用 PostgreSQL 17 作为外部数据库的初步支持。此支持仅用于测试目的，目前不支持在生产环境中使用。客户可以在非生产环境中评估 PostgreSQL 17，以便在未来全面支持之前评估其兼容性。

PostgreSQL 映像现在来自 Docker 库

从 Black Duck 2025.4.0 版本开始，PostgreSQL 映像将从 Docker 库而不是 Bitnami 获取，作为 Black Duck 的 PostgreSQL 部署的基础映像。这一过渡将自动进行，用户无需采取任何行动。

CVSS 2.0 弃用后移除 HBOM 视图

随着取消对 CVSS 2.0 的支持，Black Duck 中此前依赖于 CVSS 2.0 的 HBOM 视图将不再可用。客户应使用支持 CVSS 3.x 和 4.0 的其他报告和风险评估视图来确定漏洞优先级。

数据库迁移通知

此版本包括与漏洞修复状态处理相关的数据库迁移（详情请参见发行说明“已修复问题”部分中的 HUB-44855）。对于拥有大型数据库的客户，迁移过程可能需要一小时或更长时间才能完成。无需采取任何措施，但我们建议在升级过程中规划额外的迁移时间。

新增和更改的功能

新的 MFA 密钥过期功能

Black Duck 现在会为 MFA 密钥强制设定有效时间 (TTL)，确保它们在两分钟后或在通过 API 请求新的密钥时过期。如果用户试图使用过期或失效的密钥设置 MFA，系统将返回 401 未经授权错误和相应的消息。可对过期时间进行配置，以提高灵活性。

新的 BDSA 漏洞标签

Black Duck 现在包括两个新的 BDSA 漏洞标签，以帮助进一步分类和评估远程代码执行风险：

- 潜在的远程代码执行：标记在特定条件下可能导致远程代码执行但尚未最终确认的漏洞。

- 需要用户输入的远程代码执行：表示该漏洞需要用户通过用户界面进行交互才能利用远程代码执行。

新增针对组件和漏洞存续时间的策略规则表达式

Black Duck 现在支持两种新的策略规则表达式，允许用户根据组件或已发布漏洞的存续时间定义规则：

- 组件发布存续时间：评估组件发布后的天数。对于避免使用新发布的组件或优先使用成熟的库非常有用。
- 发布存续时间：评估漏洞发布后的天数。这有助于识别受最近披露的漏洞影响的组件。

这两种表达式都接受以天为单位的数值，并将其与当前日期进行比较。这些新增功能为创建基于时间的风险策略提供了更高的灵活性。

此功能来自客户的建议。BD-I-13

添加对通过预定义密钥提供外部数据库凭据的支持

Black Duck 现在支持在使用外部 PostgreSQL 实例时，通过用户管理的 Kubernetes 密钥传递数据库凭据。这使客户可以避免在 values.yaml 文件中存储明文凭据。

- 新增了 Helm 图表设置 useHelmChartDbCreds。该设置默认为 true，保留了现有的行为，即 Helm 图表使用 values.yaml 中定义的值创建 <name>-blackduck-db-creds 密钥。
- 通过将此值设为 false，用户将可以手动创建和管理自己的 <name>-blackduck-db-creds 密钥。
- 用户提供的密钥必须包含以下键：
  - HUB_POSTGRES_ADMIN_PASSWORD_FILE
  - HUB_POSTGRES_USER_PASSWORD_FILE
- 如果自定义密钥无效或丢失，部署将失败。系统不会退回到使用 values.yaml 中的密码。

有关更多详细信息和示例，请参见《Kubernetes 安装指南》。

此功能来自客户的建议。BD-I-7

新增对 Ubuntu 22.04 和 24.04 的支持，终止对 Ubuntu 20.04 的支持

从 Black Duck 2025.4.0 版本开始将支持 Ubuntu 22.04 和 24.04。

由于 Ubuntu 20.04 的生命周期将于 2025 年 5 月 31 日结束，Black Duck 将在 2025.7.0 中取消对该版本的支持。使用 Ubuntu 20.04 的客户应计划升级到受支持的版本，以确保持续的兼容性。

增加了对 Docker 26.x 的支持

Black Duck 现在支持 Docker 版本 26.x。此更新可确保与最新的 Docker 运行时环境兼容，并与当前的容器平台标准保持一致。

在 BOM 组件的来源 ID 选项卡中添加了 PURL 过滤器

用户现在可以使用 PURL（软件包 URL）过滤 BOM 组件的来源 ID。此项增强功能使用户可以更容易地基于标准化软件包引用定位和区分组件标识符，从而提升可追溯性和 SBOM 浏览体验。

增强的 LTS 项目版本漏洞选项卡

LTS 项目版本的“漏洞”选项卡现在包含几项更新，可提高可用性和对风险的可见性：

- 新的风险概况栏 - 可视化摘要按严重程度（严重、高、中、低）显示漏洞总数，帮助用户快速评估项目版本的整体安全态势。
- 新的搜索栏和经过扩展的过滤器 - 用户现在可以：

- 使用搜索栏按 ID、组件名称或关键词查找特定漏洞。
- 按 CWE 标签、总分、修复状态、安全风险和漏洞标签过滤漏洞。

提高导入 SBOM 时的灵活性

Black Duck 在导入 SBOM 文件时放宽了对字段的严格要求，从而提高了可用性并减少了导入错误：

- 对于 CycloneDX 报告，如果报告中缺少组件名称元数据，导入现在会成功。将使用 SBOM 的文件名作为扫描名称来代替缺少的元数据。
- 对于从 BOM 项目版本扫描页面导入的 CycloneDX 和 SPDX 报告，如果报告已映射到不同的项目版本，且用户有权限访问该项目版本，则错误消息现在会清楚地显示冲突的项目名称和版本名称，使用户更容易识别和解决映射问题。

  此行为仅在从 BOM 项目版本扫描页面导入时适用。从全局扫描页面导入时，具有相同名称的现有扫描仍会被自动替换，这种行为没有发生改变。

  如果用户没有查看其他项目版本的权限，则行为不会改变。

提高批量编辑策略规则时的性能

为了降低策略规则编辑会话期间的系统负载，Black Duck 现在限制了发布到 BOM 队列的策略规则消息的数量。以前，即使在快速或批量编辑会话中，每次保存策略规则时都会发布一条消息。这可能导致生成过多消息并影响下游性能。

通过此次更新，在集中编辑策略规则期间，会智能地减少消息发布，有助于提高系统的整体响应速度，减少对 RabbitMQ 和 PostgreSQL 等共享资源的争用。

更新策略违规通知逻辑

更新了策略违规的通知逻辑，以减少不必要的警报。现在，如果用户覆盖了策略规则违规，并且该组件后续被确定为不违规，则不会发送任何通知。以前，即使已覆盖违规，仍会触发“策略违规已清除”通知。

更新“用户和组”页面显示

“用户和组”页面已更新为在“角色”列中只显示用户的“全局角色”。以前，此列包括在项目和组级别分配的角色，在某些情况下会导致重复。此次更新可以更清晰、更准确地查看每位用户在 Black Duck 中的全局访问权限。

恢复未匹配二进制软件包管理器扫描结果的文件匹配编辑

在之前的版本中，二进制扫描的二进制文件匹配编辑被移除，以解决性能问题并提高可用性。然而，这无意中禁用了未匹配二进制软件包管理器扫描结果的文件匹配编辑，导致无法解决这些问题。本次更新恢复了对这些未匹配结果的源文件编辑，使用户可以正确管理和调整它们。

支持的最低浏览器版本

- Safari 版本 16.5
- Chrome 版本 113 (x86_64)
- Firefox 版本 112（64 位）
- Microsoft Edge 版本 113（64 位）

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

弃用 v4 和 v5 数据保留端点

Black Duck 将弃用 GET /settings/data-retention 端点的 v4 和 v5 版本，并引入 v6 作为最新版本。我们鼓励客户过渡到 v6，以利用改进的功能、性能和安全增强。

用户应该相应地更新其集成，因为 v4 和 v5 将在未来的版本中完全移除。

更新了 matched-files API 端点

以下 API 端点新增了 strict 参数。

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

默认值为 strict=true。为 true 时，响应会返回与给定组件 ID、组件版本 ID 以及空来源 ID 匹配的组件文件。如果设置为 strict=false，响应会返回与给定组件 ID、组件版本 ID 以及任意来源 ID 匹配的组件文件。

二进制扫描程序信息

二进制扫描程序已更新为版本 2025.3.0。

版本亮点和已修复的问题

- (PSC-4557)。Linux 内核未出现在 BDBA 报告中

- (PSC-4602)。Alpine 发行版针对 CVE-2025-26519 的回溯移植未生效
- (PSC-4595)。Visual_studio_runtime 与版本不匹配
- (PSC-4582)。错误的版本检测 - v8 8.17.11.962
- (PSC-4577)。Inno Setup 二进制扫描问题
- (PSC-4553)。OpenWRT .ipk 软件包无法识别为 .deb
- (PSC-4539)。ubi 文件无法在 PSC/BDBA 二进制文件中找到组件
- (PSC-4478)。组件被错误地识别为 Winsparkle
- (PSC-4468)。误报漏洞和 1 个组件匹配
- (PSC-4456)。cab 存档中的文件路径仍被混淆
- (PSC-4452)。pe32-fileinfo 版本数据未用于特征匹配。
- (PSC-4231)。二进制文件在 protecodesc 生产环境中加载时抛出错误：“扫描失败：非预期错误”

已修复的问题

此版本中修复了以下客户报告的问题：

- （HUB-34996、HUB-44573）。修复了以下问题：当漏洞与大量项目关联时，漏洞详细信息页面的“受影响项目”部分可能无法在 UI 中加载。对底层 API 查询进行了优化，以提高性能，防止超时，并确保即使对于广泛共享的漏洞，页面也能成功加载。
- (HUB-42633)。优化了 affected-bom-components API 端点的响应时间。
- (HUB-42732)。修复了以下问题：使用“全部覆盖”选项时，项目版本活动中没有正确记录的策略覆盖注释。用户现在可以根据每条策略规则输入单独的注释和覆盖到期时间。
- (HUB-43377)。修复了以下问题：“重置调整”功能可能无法对“源”页面上的手动调整条目起作用。
- （HUB-43846、HUB-43862）。改进了错误处理，以防止创建循环引用。系统现在会检测并阻止这些情况，以确保数据完整性并避免处理问题。
- (HUB-43864)。修复了以下问题：policy-status API 结果与 UI 不一致。出现这种差异的原因是在计算严重性计数时没有正确排除覆盖的策略严重性。
- (HUB-43972)。修复了以下问题：SCASS 扫描可能在轻量级 BOM 中将具有多个许可证的组件的许可证显示为未知。
- (HUB-44006)。修复了以下问题：使用直接访问（项目查看器）的用户无法在“项目组”页面上查看父项目组详细信息。
- (HUB-44177)。修复了以下问题：在对特定组件的策略违规应用“策略批准已更新”事件后，策略违规检测事件可能不会出现在“活动”窗口中。所有相关的策略事件现在都会正确记录并显示在“活动”窗口中。
- (HUB-44178)。修复了以下问题：具有多个策略违规的 BOM 组件在取消忽略后无法正确恢复所有违规。
- (HUB-44274)。修复了以下问题：不带扫描的项目版本不会被自动删除功能删除。
- (HUB-44353)。修复了以下问题：/api/vulnerabilities/<CVE>/affected-projects 页面上的“状态”列无法按预期工作。
- (HUB-44392)。修复了以下问题：即容器扫描可能会为每个映像层显示不准确的构建信息。在某些情况下（例如使用 Bazel 构建的映像），构建步骤偏移了一层，导致每一层都显示前一层的元数据。这不会影响扫描内容的准确性，但在查看层历史记录时可能会造成混淆。
- (HUB-44396)。修复了以下问题：具有重复层的容器可能生成 IncorrectResultSizeDataAccessException 错误消息。

- （HUB-44408、HUB-44590）。修复了以下问题：包含日文和其他特殊字符的源代码无法上传，并生成 The content type is not allowed 错误消息。
- (HUB-44506)。修复了以下问题：Gen05 规模调整 yaml 文件中容器的“HUB_MAX_MEMORY”变量缺失。
- (HUB-44551)。修复了以下问题：在查看项目组的设置时，导航到新项目组的设置会显示之前查看的项目组数据。
- (HUB-44604)。修复了以下问题：当 BD 部署了时区设置时，许可证过期日期的 UTC 时间被视为本地时间，导致过期时间早于实际许可证时间。
- (HUB-44649)。修复了以下问题：在代码段匹配中显示的文件匹配数量翻倍。
- (HUB-44670)。修复了以下问题：部分配置的 mTLS 设置可能会错误地将空证书字段视为有效，从而在数据库连接期间导致意外行为。现在只包含正确配置的证书。
- （HUB-44674、HUB-44970）。修复了以下问题：在扫描期间使用 --detect.clone.project.version.name 参数时，未正确从指定的项目版本复制设置。
- (HUB-44706)。修复了以下问题：如果漏洞的 CVSS4 向量不包含“漏洞利用成熟度”值，则在创建版本详细信息报告时，可能会产生 NullPointerException 错误。
- (HUB-44747)。修正了 Black Duck 生成的 SPDX SBOM 中 creationInfo 部分的创建者字段格式。以前，工具名称和版本用连字符分隔，周围没有空格，这不符合 SPDX 规范。现在的格式按要求在连字符两侧各包含一个空格。
- (HUB-44820)。修复了以下问题：快速扫描在某些情况下可能会遗漏某些漏洞。快速扫描中使用的评分逻辑已更新，从而与完整扫描保持一致，确保在各种扫描类型中保持漏洞检测的一致性（尤其是在使用 CVSS v4 或更新排名配置的环境中）。
- （HUB-44853、HUB-44876）。解决了以下问题：组件的“安全”选项卡可能会显示漏洞计数，但在列表中却显示“无结果”。这是由于在确定漏洞优先级时应用 CVSS 版本的方式不一致造成的。显示逻辑已得到修正，以确保漏洞数据的显示与报告的计数一致。
- (HUB-44855)。修复了以下问题：漏洞修复状态错误地应用于组件版本的所有来源，而不是只应用于预期的那一个来源。系统现在会正确地反映每个来源的修复状态。请注意，此修复包括数据库迁移。对于拥有大型数据库的客户，迁移可能需要一小时或更长时间才能完成。
- (HUB-44872)。修复了以下问题：具有项目经理或项目管理员角色的用户无法删除 LTS 版本。
- (HUB-44879)。修复了以下问题：“检测到策略违规”事件通知在重新扫描后可能意外重新触发，导致创建 Alert 重复 JIRA 注释。
- (HUB-44889)。修复了 UI“?”下拉菜单中损坏的 Black Duck 教程链接。
- (HUB-44891)。修复了以下问题：标记为忽略的组件会继续在“组件”选项卡上显示安全风险指标。被忽略的组件现在将正确排除安全风险数据。
- (HUB-45007)。修复了以下问题：在未指定组件版本的情况下，用户无法保存代码段匹配，从而产生“无法在没有版本 ID 的情况下创建/修改对项目的文件调整”错误。

Black Duck SCA 2025.1.x

Black Duck 2025.1.1

公告

目前尚未发布有关 Black Duck 2025.1.1 的新公告。

新增和更改的功能

新增对 IPv6 入口和出口通信的支持

Black Duck 现在支持用于内部和外部通信的 IPv6 专属网络。此增强功能确保了与仅 IPv6 环境的兼容性，实现了 Black Duck 组件、KnowledgeBase、客户系统和面向互联网的网络 Pod 之间的无缝通信。

在 component_vulnerability 表中添加了 justification 字段

报告数据库中的 component_vulnerability 表添加了新的 justification 字段。该字段可存储漏洞的理由详细信息，为修复决策和分析提供额外的上下文信息。

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

2025.1.1 中没有新增或更改的 API 请求。

二进制扫描程序信息

Black Duck 2025.1.1 中的二进制扫描程序没有更新。

有关更改的完整列表，请参阅Black Duck 二进制分析发行说明。

已修复的问题

此版本中修复了以下客户报告的问题：

- (HUB-43061)。修复了以下问题：在扫描 .js 文件时，使用 --detect.blackduck.signature.scanner.individual.file.matching=SOURCE 选项可能导致无结果。
- (HUB-43374)。为 V8 /api/projects/{projectId}/versions/{projectVersionId}/vulnerable-bom-components 端点添加了缺失的描述、源和严重性字段。
- （HUB-43389、HUB-44090）。修复了以下问题：当安全风险的漏洞状态设置为已忽略/已缓解/修复完成时，该安全风险仍被计入 BOM。
- (HUB-43931)。修正了以下问题：组件可能无法合并到项目的“源”选项卡中。
- (HUB-44076)。修复了以下问题：将 Black Duck 从版本 2023.1.2 更新到 2024.4.1，以及将 Alert 从版本 6.12.2 更新到 7.2.0 后，访问 https://HUB_URL/alert/ 时可能显示空白页。
- (HUB-44089)。修复了以下问题：已删除组件中的安全漏洞仍显示在项目的“安全性”选项卡中。
- (HUB-44104)。修复了以下问题：代码段匹配在被修复为“已确认”并随后在“源”选项卡上标记为“已忽略匹配”后，仍会在“BOM”和“源”选项卡中显示策略违规。
- (HUB-44185)。修复了可能导致“新增功能”窗口空白的代理问题。
- (HUB-44186)。修复了更新 version_bom_risk_profile 时可能出现的数据库死锁问题。
- (HUB-44190)。修复了以下问题：对于映射了 CycloneDX SBOM 的项目，SPDX 报告生成可能会失败。
- (HUB-44210)。修复了以下问题：在 BOM 中展开“源”树可能导致“400 错误请求”错误。
- (HUB-44253)。修复了更新 version_bom_component 时可能出现的数据库死锁问题。
- (HUB-44365)。修复了以下问题：在将使用 cyclonedx-cli 工具合并的 CycloneDX SBOM 导入单个 SBOM JSON 文件时，可能产生重复键错误。
- (HUB-44366)。修复了以下问题：版本报告端点的 REST API 文档的 aggregateBomViewEntries 数组中不再包含“scan”数组。
- (HUB-44486)。修复了以下问题：当基础映像层和自定义层中出现相同的组件标识符时，容器扫描中的组件匹配会被错误地存储。
- (HUB-44515)。将 Detect Desktop 迁移到了 Black Duck，包括下载链接和品牌标识。
- (HUB-44549)。修复了以下问题：运行 apt 更新后，容器扫描可能生成不同的结果。
- （HUB-44584、HUB-44623）。修复了以下问题：blackduck-postgres-init 作业在托管环境中可能会失败，从而阻碍成功执行 Create Hub 作业。

Black Duck SCA 2025.1.0

公告

新 Gen05 规模指南

Black Duck 已升级到 Gen05 规模，在资源优化方面实现显著的改进。新的硬件建议可将效率提高 25% 至 45%，确保现代工作负载的可扩展性和性能得到增强。我们建议客户查看更新后的硬件要求，以便充分利用这些优化。

Detect 10 发布，Detect 8 支持终止

Detect 10 现已推出，提供增强的功能和改进。作为此次发布的一部分，对 Detect 8 的支持将于 2024 年 10 月 31 日终止。

主要变化包括：

- 已配置 Detect 8.x 的客户在升级时会看到红色警告指示器，建议他们迁移到受支持的版本。如果用户尝试从 Detect 8.x 切换到其他版本，因为这个操作是不可逆的，所以也会显示一个警告。
- 新安装将不再提供 Detect 8.x 选项。
- 对于升级，只有之前已配置 Detect 8.x 的客户才可以看到该选项。
- 对于新客户或升级到版本 2025.1.0 且之前未设置 Detect 属性的情况，Detect 10 现在将成为默认选项。

即将弃用项目版本分层材料清单

Black Duck 中的项目版本分层材料清单 (BOM) 功能计划在版本 2025.4.0 中弃用。建议依赖此功能的用户开始迁移到替代工作流程，以确保流程不会中断。

新增和更改的功能

可用于 SCA 扫描服务 (SCASS) 的新扫描类型

SCA 扫描服务 (SCASS) 已得到增强，现在包括对二进制和容器扫描的支持。此更新扩展了该服务的功能，为管理不同扫描需求的用户提供了更广泛的分析并提高了灵活性。

添加了新的修复状态

Black Duck 现在包括网络安全和基础设施安全局 (CISA) 所描述的 VEX（漏洞利用交换）修复状态值。这些值提供对漏洞的可利用性和修复工作的详细跟踪，帮助您更有效地评估和管理漏洞风险。添加了以下修复状态值：

- 已知受影响 (AFFECTED)：建议采取措施来修复或解决此漏洞。
- 已知不受影响 (NOT AFFECTED)：必须提供理由来确保妥善记录该决定。
- 正在调查中 (UNDER INVESTIGATION)：目前尚不清楚这些产品版本是否受到该漏洞的影响。将在后续版本中提供更新。

为组件版本定义默认 CPE 的新功能

Black Duck 现在能够为组件版本定义默认的通用平台枚举 (CPE)。此功能可通过确保一致的 CPE 与每个组件版本关联来简化漏洞跟踪，从而减少对手动更新的需求。用户可以直接在组件版本设置中配置默认 CPE，简化 SBOM 生成并提高数据准确性。

用于 BOM 组件信息的新滑出式面板

在项目版本的“组件”选项卡中，现在单击组件会打开滑出面板，而不是导航到新页面。此更新保留了组件使用的上下文，无需在页面之间来回切换即可获取其他信息。

SBOM 模板中添加了新的排除未确认代码段匹配选项

SBOM 模板的“组件数据”部分添加了新的 SBOM 模板选项“排除未确认的代码段匹配”。用户可以利用此选项从其 SBOM 中排除具有未经确认代码段匹配的组件，从而更清晰、更精确地表示项目的开源组成。

新扫描 CSV 数据

Black Duck 现在支持使用扫描 CLI 中的新 --upload-csv 参数在扫描期间生成 CSV 数据。借助此功能，用户可以在扫描期间创建 CSV 文件并自动将其上传至 Black Duck。此外，用户可以直接从 Black Duck 界面中的“扫描”页面和项目版本的“设置”选项卡下载 CSV 数据，从而灵活地访问扫描结果以进行进一步分析和报告。

增加了对 CycloneDX 1.6 的支持

您现在可以用 CycloneDX v1.6 格式导出项目的软件材料清单报告。这可以通过查看项目版本，单击“报告”选项卡，单击“创建报告”按钮，然后选择 CycloneDX v1.6 — JSON 来完成。有关 CycloneDX v1.6 的更多信息，请访问 CycloneDX v1.6 参考页面。

增加了对 CVSS v4.x 漏洞评分排名的支持

Black Duck 现在包括对 CVSS（常见漏洞评分系统）4.0 版的支持，为基本指标提供增强的粒度、新的补充指标组、用于确定严重性的更新方法以及其他改进。有关 CVSS v4.0 的更多详细信息，请访问官方规范文档，地址为：https://www.first.org/cvss/v4.0/specification-document。

增加了对 SAML 签名的身份验证证书的支持

Black Duck 现在支持 SAML 签名的身份验证证书，通过根据受信任的证书验证身份验证请求来增强安全性。系统管理员可以直接在 SAML 配置设置中管理证书。

默认情况下启用更新的 JWT 会话令牌失效

现已默认启用注销时使 JWT 会话令牌失效的功能。此更新确保在用户注销后会话令牌不再有效，从而增强安全性。

停止支持 CVSS v2 漏洞分数排名

不再支持 CVSS v2 作为最高优先级的 CVSS 排名。但如果漏洞不存在 CVSS v3.x 或 CVSS v4.x 分数，则仍会显示 CVSS v2 分数。

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

删除了对 access_token 请求参数的支持

为了解决安全漏洞，不再支持通过 access_token 请求将授权令牌 (JWT) 作为请求参数来传递。用户应确保使用授权 HTTP 标头传递授权令牌，如 REST API 开发人员指南中所述。

二进制扫描程序信息

二进制扫描程序已更新为版本 2024.12.2。

版本亮点

- 增加了对 ARM64 架构的支持
- 更新了 NET 扫描程序：
  - 减少了 BOM 中未知版本组件的数量，从而减少了手动分类的工作量
  - 更准确地反映 .NET 组件结构

有关更改的完整列表，请参阅Black Duck 二进制分析发行说明。

已修复的问题

此版本中修复了以下客户报告的问题：

- (HUB-39655)。修复了 Kubernetes 部署中的问题：当 Logstash 磁盘因活动频繁而填满时，Black Duck webapp 会进入崩溃循环。为了解决这个问题，我们实施了日志删除脚本来管理 Logstash 磁盘使用情况。
- (HUB-42725)。修复了以下问题：“通知”页面上的分页标签可能无法显示页面上的实际通知数。
- (HUB-43212)。修复了以下问题：对 maxRamPercentage 设置的更改仅适用于 Gen04 规模，导致使用 Gen02 规模的托管客户出现问题。
- (HUB-43295)。修复了“查找”页面 →“漏洞”选项卡上的问题：“使用者”部分显示错误的项目版本。
- (HUB-43394)。修复了以下问题：UI 为与许可证状态相关的策略条件显示“有条件批准”，而不是显示“有限批准”。这些术语现在在整个平台上保持一致。
- (HUB-43426)。修复了以下问题：分区日志会相互重叠。
- (HUB-43431)。为 upload-cache-source-migrator.pl 脚本增加了更高的容错能力，从而在出现错误时记录错误信息并继续执行后续操作。
- (HUB-43556)。修复了以下问题：将过滤器从“总计已更改”更改为“新组件”后，项目版本比较视图无法显示任何结果。
- (HUB-43560)。修复了以下问题：具有项目创建者角色（指定为单个项目组的经理）的用户能够在组之间移动任何项目。现在，这些用户受到适当的限制，只能移动他们创建的项目。
- (HUB-43791)。修复了以下问题：尽管 PUT /api/projects/{projectId} 端点只需要项目的 name 参数，但它要求存在 projectOwner 参数/值。
- (HUB-43826)。修复了 GET /api/projects/{projectId}/versions/{projectVersionId}/reports/{reportId}/contents 端点的问题：显示错误消息，指出文件大小的最大限制仅适用于 HTML 报告。该消息现在还包括 JSON 流。

- (HUB-43839)。修复了以下问题：未确认代码段策略使用“查找”页面中的优先级标签未返回结果。
- (HUB-43841)。修复了以下问题：在“设置”→“版本详细信息”选项卡下将许可证添加到项目版本，然后生成 SBOM 报告时，提取的文本会显示为“无”。
- (HUB-43847)。修复了以下问题：组件名称中的特殊字符会导致安全选项卡返回零漏洞结果。
- (HUB-44004)。修复了以下问题：将带有版本的子项目更新为带有未知版本的子项目会在 BOM 中生成错误。
- (HUB-44114)。修复了以下问题：/api/projects/{projectId}/versions/{projectVersionId}/components 端点允许在没有指定版本的情况下将项目添加到 BOM。
- (HUB-44184)。修复了组件批量编辑窗口中的问题：在显示所选项目数量时，窗口中显示“{count}”，而不是显示 Black Duck 日语本地化中的实际数字。

Black Duck SCA 2024.10.x

Black Duck 2024.10.1

公告

增加了对 ARM64 架构的支持

Black Duck 现在包括对 ARM64 架构的支持，从而将兼容性扩展到更广泛的系统和环境。ARM64（也称为 AArch64）广泛用于现代服务器平台，包括基于 ARM 的云环境（如 AWS Graviton），以及应用于嵌入式和 IoT 设备。此更新确保运行基于 ARM64 的系统的用户可以利用 Black Duck 的功能有效地进行开源风险管理。

请注意，从 2024.10.1 开始，ARM 系统不再支持 BDBA 和 RL 服务。计划在版本 2025.1.0 中提供 BDBA 支持，但目前尚未计划支持 RL 服务。

新增和更改的功能

用于软件包管理器和特征扫描的新 SCA 扫描服务

Black Duck 现在提供 SCA 扫描服务 (SCASS)，这是一个可扩展的解决方案，用于在传统 Black Duck SCA 环境之外执行软件组成分析扫描。SCASS 支持软件包管理器和特征扫描，使其成为可满足各种扫描需求的多功能选择。

该服务为本地客户和托管客户提供了显着的优势：

- 本地客户：大大减少了对非专业扫描的资源需求，从而简化了基础设施需求。
- 托管客户：根据总体扫描需求进行动态扩展，提高云基础设施效率，从而提高性能并降低运营开销。

SCASS 还支持关联扫描，这是一项新功能，利用 SCASS 通过结合多种扫描技术的见解来增强匹配结果。

此外，SCASS 可以更快地交付扫描错误修复，与 Black Duck 发布周期无关。虽然扫描结果以事务方式存储，但这种简化的服务增强了跨平台扫描的灵活性和可扩展性。

请注意，必须在您的产品注册密钥中启用此功能才能利用该服务。借助 SCASS，您可以简化资源管理并获得更具可扩展性的扫描体验。请联系您的 Black Duck 代表以了解更多信息。

LTS 漏洞视图中的新排序功能

LTS 漏洞视图现在包括排序功能，使您可以按以下标准来整理漏洞，从而改进导航和分析：

- 漏洞 ID（默认）

- 受影响的组件，列表中的第一个组件
- 总体得分
- 修复状态

“项目设置”页面添加了新的 URL 字段

“项目设置”页面中添加了新的 URL 字段，用于在项目版本用作父项目中的组件时定义 SBOM 中的主页值。

- 如果在模板中启用，则 URL 字段用作 SBOM 中的主页。
- 对于新项目，除非已从具有预填充 URL 的项目克隆该字段，否则该字段为空。
- 相同的 URL 适用于所有项目版本；不能在 BOM 组件级别覆盖。

从 BOM 中删除的软件包管理器匹配的匹配置信度

材料清单 (BOM) 中不再包括软件包管理器匹配的匹配置信度分数。此更新反映了软件包管理器匹配的固有准确性，不太可能出现歧义。匹配置信度继续应用于其他类型的组件匹配。

合并的 Kubernetes 和 Openshift 安装指南

之前分开的 Kubernetes 和 Openshift 安装指南已合并为一个统一的指南。这个精简的文档将所有相关说明整合到一处，从而简化了安装过程。请注意，Swarm 安装指南仍作为单独的文档进行维护。

更新了二进制和容器扫描的最大上传大小更改

从 Black Duck 2024.10.0 开始，客户现在可以通过调整 BINARY_UPLOAD_MAX_SIZE 环境变量，将二进制和容器扫描的最大上传大小从默认的 5 GB 增大到 100 GB。该文档已更新为体现这个新的配置更改。

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

增加了对 LTS 漏洞查看端点的排序

GET /api/lts-projects/{projectId}/lts-project-versions/{versionId}/vulnerabilities API 端点现在支持按以下几点排序：

- 漏洞 ID（默认）
- 受影响的组件，列表中的第一个组件
- 总体得分
- 修复状态

二进制扫描程序信息

二进制扫描程序已更新为版本 2024.9.1。有关此版本的更多信息，请参阅 Black Duck 二进制分析 发行说明。

已修复的问题

此版本中修复了以下客户报告的问题：

- (HUB-43265)。修复了以下问题：在克隆项目时，如果选择了用户和组，而没有为该项目分配任何用户组，就会生成“HTTP 400 — 参数集为空”的堆栈跟踪错误。
- (HUB-43391)。修复了以下问题：SBOM 报告中仍包括已忽略的组件/子项目。
- (HUB-43413)。修复了以下问题：设置“有注释的组件”过滤器时，有时会出现没有注释的组件。
- (HUB-43588)。修复了以下问题：更改组件的许可证后，“组件”页面顶部的许可证风险计数没有立即更新，有时需要几天时间才能反映更改。
- (HUB-43760)。修复了以下问题：字符串“(c) Copyright”会导致版权规范化作业失败。
- (HUB-43860)。修复了以下问题：由于视图定义不匹配，bds_hub 的数据库转储无法还原。

Black Duck SCA 2024.10.0

公告

Black Duck SCA 现已成为 Black Duck 的一部分，后者是完全独立于 Synopsys 的实体

通过此次更新，您将注意到品牌的变化，包括新的 Black Duck 徽标。如需了解更多信息，请参阅 Black Duck 独立启航。

此外，我们还推出了新的网站和社区门户。请更新您保存的任何 Black Duck 文档和书签。有关新 URL 的详细信息，请参阅 Black Duck 域变更常见问题解答。

在此过程中，sig-repo.synopsys.com 将被逐步淘汰。请改用 repo.blackduck.com。我们建议将 sig-repo.synopsys.com 保留在您的允许列表中，直到 2025 年 2 月它被 repo.blackduck.com 完全取代。

引入基于上限的速率限制策略

从 2025 年第一季度开始，我们将开始推出基于上限的速率限制策略。预计此项变化在初期影响较小，并可能首先针对 Black Duck 托管客户推出。

- Black Duck 将密切监控此次推出，并对达到上限阈值的客户采取必要的措施。
- API 流量负载较高的客户在重度使用的场景下可能会遇到速率限制。如果您遇到 HTTP 429 - Too Many Requests 响应，我们强烈建议您在构建自定义 API 集成应用程序时，实施减少 API 流量的策略。

Java 开发工具包 (JDK) 升级到版本 17

Black Duck 2024.10.0 版本已从使用 JDK 11 升级到使用 JDK 17。此次升级带来了更强的性能、更高的安全性和长期支持，确保为托管产品和本地产品提供更稳健、更适合未来发展的环境。

使用这两个版本的用户和开发人员应确保其环境与 JDK 17 兼容，以充分利用此次升级。

即将弃用 BDIO1

请注意，从 2025.1.0 版本开始，BDIO 文件的 BDIO1 格式将被弃用。Detect 版本 8 及更高版本使用 BDIO2 和后续版本，只有不受支持的 Detect 版本才会继续使用 BDIO1。

BDIO (Black Duck I/O) 文件基于 JSON，用于存储扫描结果，包括项目中的开源组件、依赖关系、漏洞和许可证。它们能够在 Black Duck 扫描程序和平台之间进行高效数据传输，以便进一步分析，并集成到开发工作流程中。

对于运行 Black Duck 早期版本并且仍使用 BDIO1 的客户，我们将在这些版本中继续支持 BDIO1。如果您修改 BDIO1 文件，这些修改仍将与 Black Duck 2024.10.0 或更早的版本保持兼容。但是，当升级到 Black Duck 2025.1.0 或更高版本时，您需要更新您的修改，与 BDIO2、BDIO3 或更新版本兼容。

对 BDIO2 和 BDIO3 的支持没有变化；两者都将继续得到全面支持。

终止对 PostgreSQL 14 的支持

随着 2024.10.0 版本的发布，Black Duck 将结束对外部 PostgreSQL 14 的支持。有关更多信息，请参阅 PostgreSQL 版本升级计划页面。

针对 PostgreSQL 容器用户的升级限制

对于 Black Duck 提供的 PostgreSQL 容器的用户，Black Duck 2024.10.0 仅支持从使用 PostgreSQL 13 或 14 容器的早期 Black Duck 版本（包括 2022.10.0 至 2024.7.x）直接升级。

从旧的 Black Duck 版本（2022.10.0 之前）升级需要两步升级：

1. 升级到 Black Duck 2023.7.x。
2. 升级到 Black Duck 2024.10.x。

PostgreSQL 容器迁移到版本 15

Black Duck 会在 2024.10.0 版本中将其 PostgreSQL 映像迁移到版本 15。不使用 Black Duck 提供的 PostgreSQL 映像的客户不会受到影响。

关于二进制扫描性能指标

当二进制扫描量占总扫描量（按扫描次数计算）的 20% 或更少时，Black Duck 硬件扩展指南上提供的此指南有效。性能测试指标应作为扩展服务器的指导原则。并非所有具有一定大小的二进制文件都相同，因为二进制文件中发现的提取层数和已识别组件数量所需的资源可能比性能测试中确定的更多，也可能要少。

新增和更改的功能

多因素身份验证 (MFA) 的新功能

Black Duck 2024.10.0 版本现包含一项多因素身份验证 (MFA) 的新功能，可增强用户帐户的安全性。启用 MFA 后，用户将使用 MFA 令牌、基于短信或应用程序的验证码进行第二层验证。这一额外步骤有助于确保只有授权用户才能访问系统，可进一步保护敏感数据。

新的关联扫描

Black Duck 2024.10.0 版本添加了一种新的扫描方法，它将软件包管理器和签名扫描的匹配结果关联起来，以增强扫描结果。通过整合不同扫描方法的优势并弥补其不足，关联扫描可有效减少误报和版本扩散。这些扫描方法之间的关联可确保获得更准确、更全面的结果。

Black Duck 2024.10.0 版本仅支持单个签名扫描和一个/多个软件包管理器扫描结果之间的关联。不建议将其与其他扫描类型一起使用。

组件版本页面新增“来源 ID”选项卡

组件版本页面新增了“来源 ID”选项卡。此选项卡列出了与特定组件版本相关的所有已知外部 ID 和软件包 URL (PURL)，为每个组件的来源提供了更详细的可见性。

新的文件调整简化

文件调整过程已简化为使用基于路径的调整，而不是基于签名的调整。这一变化改善了用户体验，提高了性能，并消除了在 KnowledgeBase 中推进基于签名的组件匹配的障碍。例如，如果同一文件、目录或存档出现在多个位置（如映射到同一项目版本的不同代码位置），则只会调整一个实例。

登出后新会话令牌失效

这项新功能实现了在用户登出系统后使会话令牌失效。这可以确保令牌在登出后无法重复使用，从而提高安全性。但是，此功能在默认情况下未启用。要激活它，管理员必须配置 blackduck-config.env 文件，并将 JWT_BLOCK_LIST_CHECK 变量设为 true。

更新了外部身份验证配置位置

SAML 和 LDAP 的外部身份验证配置页面已从“管理”→“系统设置”→“用户身份验证”移至“管理”→“集成”→“外部身份验证”。

此外，“用户身份验证”页面已重命名为“本地身份验证”，以反映其更新的功能。

更新了对将多个容器扫描映射到单个项目版本的支持

我们增强了系统，允许将多个容器扫描映射到单个项目版本。以前，每个项目版本只能映射一个容器扫描。此增强功能为跨不同容器管理和分析代码库提供了更高的灵活性。以下是可映射到单个项目版本的扫描（代码位置）的有效组合：

- 映射到项目版本的非容器扫描的任意组合。
- 映射到项目版本的一个或多个容器扫描。
- 映射到同一项目版本的一个或多个容器扫描，以及一个或多个 IaC/恶意软件扫描。

映射代码位置的所有其他组合均无效，如果相应代码位置的映射将导致无效组合，则扫描过程将失败。

在本次更新中，需要进行迁移，以更改容器名称的构造方式。以前，容器名称根据其代码位置派生。今后，它们将根据 BDIO 文件中提供的容器 tar 文件 URI 生成。

为 LTS 项目添加了漏洞修复功能

长期支持 (LTS) 项目现在支持设置漏洞修复状态，帮助团队跟踪和记录项目中漏洞的解决过程。

更新了速率限制配置

为提高系统整体性能，Black Duck 中默认禁用速率限制。如过需要，仍可通过将 BLACKDUCK_USE_HEAP_RATE_LIMITING 环境变量设置为 ON.手动重新启用速率限制。

支持的最低浏览器版本

- Safari 版本 16.1
- Chrome 版本 107 (x86_64)
- Firefox 版本 106（64 位）
- Microsoft Edge 版本 107（64 位）

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

多因素身份验证 (MFA) 的新端点和更新端点

在多因素身份验证 (MFA) 的新功能中，引入了以下新的 API 端点：

- 获取当前用户 MFA 密钥

  GET /api/current-user/mfa
- 为当前用户设置 MFA

  POST /api/current-user/mfa
- 重置当前用户的 MFA

  DELETE /api/current-user/mfa
- 为用户重置 MFA

  DELETE /api/users/{userId}/reset-mfa
- 为当前用户验证 MFA

  POST /api/mfa/authenticate

此外，还更新了以下端点的响应，以包含有关每个用户是否已设置多因素身份验证 (MFA) 的信息。

- 列出用户

  GET /api/users
- 读取当前用户

  GET /api/current-user

更新 users 和 current-user 端点

GET /api/users 和 GET /api/current-user 端点响应已更新，以包含有关每个用户是否已设置多因素身份验证 (MFA) 的信息。

用于容器多部分上传的新端点

引入了新的 API 端点，以通过容器多部分上传增强文件上传过程。通过这些端点，您可以将大文件分成小块上传，从而提高效率和可靠性。这些新端点包括：

- 开始上传

  POST /api/storage/containers/{container_id}/multipart
- 上传文件的部分

  PUT /api/storage/containers/{container_id}/multipart
- 完成上传请求

  POST /api/storage/containers/{container_id}/multipart/completed
- 取消上传请求

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

有关详细的使用和有效载荷说明，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

SBOM 字段 API 停用通知

自 Black Duck 2024.10.0 版本起，以下三个 SBOM 字段 API 已停用，并将返回无内容的 410 GONE 响应：

- 列出 SBOM 字段范围

  GET /api/sbom-fields/scopes
- 列出范围内的 SBOM 字段

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

- 更新 SBOM 字段的状态

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

这些 API 也已从《REST API 开发人员指南》中移除，并将在即将发布的版本中完全移除。

已弃用的 LTS API 端点

以下 LTS API 端点已被弃用，并将在即将发布的版本中移除：

- 通过 projectId 更新 LTS 项目

  PUT /api/lts-projects/{projectId}

  可以通过 PUT /api/projects/{projectId} 端点更新 LTS 项目。

- 通过 projectId 删除 LTS 项目

  DELETE /api/lts-projects/{projectId}

  可以通过 DELETE /api/projects/{projectId} 端点删除 LTS 项目。

- 更新 LTS 项目版本

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

  可以通过 PUT /api/projects/{projectId}/versions/{projectVersionId} 端点更新 LTS 项目的版本信息。

添加了指向 API 端点的 HATEOAS 链接

以下端点已更新，以在其响应中包含 HATEOAS 链接。这些链接提供了动态导航，允许客户端发现可用的操作或相关资源，无需硬编码 URL。

- 更新项目版本的 BOM 状态

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

- 读取 LTS 项目

  GET /api/lts-projects

- 通过 projectId 读取 LTS 项目

  GET /api/lts-projects/{projectId}

- 通过 projectId 更新 LTS 项目

  PUT /api/lts-projects/{projectId}（已弃用）

- 通过 projectId 删除 LTS 项目

  DELETE /api/lts-projects/{projectId}（已弃用）

尽管其中两个端点已被弃用，但在非弃用端点更新的过程中，它们也收到了 HATEOAS 链接。虽然此次更新主要针对活动端点，但由于共享响应格式的原因，被弃用的端点也受到了影响。

二进制扫描程序信息

二进制扫描程序已更新为版本 2024.9.1。有关此版本的更多信息，请参阅 Black Duck 二进制分析 发行说明。

已修复的问题

此版本中修复了以下客户报告的问题：

- (HUB-33532)。修复了以下问题：在“版本详细信息”报告中，当查看报告内容时，未正确转义的反斜杠字符可能导致 JSON 格式无效的错误。
- (HUB-36358)。修复了以下问题：Signature Scanner 在扫描使用 Pack200 格式压缩的文件时可能失败。出现该问题的原因是 Apache Commons Compress 库的新版本引发了不兼容。通过对该库进行本地更新，该问题已得到解决。
- (HUB-41944)。修复了以下问题：修改特定组件版本的自定义字段时，组件详细信息选项卡中的“已更新”字段未反映更改，但正确反映组件版本详细信息和许可证的更改。
- (HUB-42604)。修复了以下问题：BOM 的“组件”页面上显示的匹配计数与“来源”页面上显示的计数不同。
- (HUB-43043)。修复了以下问题：在审查/取消审查组件、更改组件版本/许可证、忽略/取消忽略组件、手动添加组件、添加注释、确认/编辑/忽略代码段匹配后，BOM 页面会自动刷新。该表现在仍会刷新，但在后台不再消失。
- (HUB-43170)。修复了以下问题：遇到无效存档文件时，Signature Scan 可能会在 cli 输出中生成 java.nio.file.InvalidPathException 警告消息。
- (HUB-43220)。优化了许可证 API 端点（ /api/internal/composite/licenses/{licenseId}/usages 和 /api/licenses/{licenseId}/bom-counts ）中使用的查询，该查询会导致加载时间超出预期。
- (HUB-43307)。在 Black Duck 中将 OpenJDK 版本更新至 Zulu Java 17.0.12，以解决漏洞问题。
- (HUB-43315)。修复了在升级到 Black Duck 2024.7.0 版本后，与生成报告时提取版权信息的查询相关的性能问题。
- (HUB-43342)。修复了以下问题：添加到许可证的备注未显示在 BOM 许可证详细信息中。我们将在可折叠元素的“备注”部分显示这些备注，并在备注较长时提供显示更多/显示更少按钮。如果许可证没有添加任何备注，则不会出现“备注”部分。
- (HUB-43382)。修复了以下问题：二进制扫描的源文件调整可能影响多个文件，二进制文件和 JAR 文件中都会显示匹配结果。现在已禁用二进制扫描的源文件调整。
- (HUB-43389)。修复了以下问题：取消映射扫描后，在重新映射时，风险警告数据未被保留。
- (HUB-43502)。在 version_bom_applied_adjustment 表上创建了新索引，以提高更新许可证文本时的性能。

Black Duck SCA 2024.7.x

Black Duck 2024.7.3

公告

Black Duck SCA 现已成为 Black Duck 的一部分，后者是完全独立于 Synopsys 的实体

通过此次更新，您将注意到品牌的变化，包括新的 Black Duck 徽标。如需了解更多信息，请参阅 Black Duck 独立启航。

此外，我们还推出了新的网站和社区门户。请更新您保存的任何 Black Duck 文档和书签。有关新 URL 的详细信息，请参阅 Black Duck 域变更常见问题解答。

在此过程中，sig-repo.synopsys.com 将被逐步淘汰。请改用 repo.blackduck.com。我们建议将 sig-repo.synopsys.com 保留在您的允许列表中，直到 2025 年 2 月它被 repo.blackduck.com 完全取代。

新增和更改的功能

Black Duck 2024.7.3 中没有新增或更改的功能。

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

Black Duck 2024.7.3 中没有新增或更改的 API 端点。

二进制扫描程序信息

二进制扫描程序已更新为版本 2024.6.3。有关此版本的更多信息，请参阅 Black Duck 二进制分析 发行说明。

已修复的问题

此版本中没有修复客户报告的错误。

Black Duck SCA 2024.7.2

公告

目前尚未发布有关 Black Duck 2024.7.2 的新公告。

新增和更改的功能

新的安全 JWT 密钥对配置

我们增强了 JWT 处理功能，允许安全地预置公钥/私钥对，从而提高整体安全性和运行效率。此配置是可选的，不是部署的必需条件。您现在可以将这些密钥对安全地提供给需要它们的服务，而不是自动生成并存储在数据库中。

目前，仅支持 RSA 密钥（PEM 编码）。具体来说，公钥必须采用 X.509 格式，私钥必须采用 PKCS#8 格式。签发 JWT 的服务（如身份验证服务）主要需要私钥，而提供需要授权访问的公共 API 的任何服务都需要公钥。

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

更新了代码段匹配 API

已更新 POST /api/snippet-matching API 请求，以接受通过 Black Duck 向客户提供的算法从源代码生成的指纹。

二进制扫描程序信息

二进制扫描程序已更新为版本 2024.6.3。

已修复的问题

此版本中没有修复客户报告的错误。

Black Duck SCA 2024.7.1

公告

目前尚未发布有关 Black Duck 2024.7.1 的新公告。

新增和更改的功能

更新了组件来源版权对话框

目前，我们会在“组件来源版权”对话框中显示 kbCopyright 文本，但仅在版权被修改时显示。通过此更新，我们将在现有文本块下方的第二个文本块中始终显示完整的版权文本，并标注“完整版权文本”以供参考。此信息不可编辑。

带有 LTS 版本指示器的增强型仪表板

仪表板已得到增强，包括具有长期支持 (LTS) 版本的项目的指示器。用户现在可以更轻松地直接从仪表板识别哪些项目具有 LTS 项目版本，这提高了长期支持项目的可见性和可管理性。

带有外部 ID 的增强型 BOM 组件选项卡

BOM 组件选项卡现在将利用新的 inputExternalIds 字段为二进制和容器匹配提供更多有用信息。当前消息已更新，并将在组件出现以下情况时显示：

- matchTypes 包含二进制文件。
- componentVersion 在组件的响应中缺失。
- origins 在组件的响应中为空。

更新后的当前消息如下（更新部分以斜体显示）：

> 未知版本
>
> 该组件的版本未知。许可证风险是估算的。要获得更准确的结果，请手动指定组件的版本。
>
> 在二进制扫描过程中发现了该标识符：
>
> <数据>
>
> 或者
>
> 在二进制扫描过程中发现了这些标识符：
>
> <数据>
>
> <数据>

对于使用 API 的用户，inputExternalIds 字段始终可用于受支持的扫描。虽然并非出现在所有扫描类型中，但在使用此功能的扫描中，它们将出现在所有 BOM 项目中。

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

风险概况仪表板请求新增 ltsReleaseCount 属性

GET /api/risk-profile-dashboard API 请求新增了一个属性。ltsReleaseCount 属性会返回转换为 LTS 的版本数量。

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

LICENSE_TEXT 和 LICENSE_DATA 类别不再添加到所有通知报告中。如果请求不包含任何类别，则默认为 LICENSE_TEXT 和 LICENSE_DATA。如果请求包含 DEEP_LICENSE_DATA 或 FILE_LICENSE_DATA，则会在请求中添加 LICENSE_TEXT 和 LICENSE_DATA。在所有其他情况下，报告将只包括 API 请求中的类别。

更新了 vulnerable-bom-components API 请求

在 GET /api/projects/{projectId}/versions/{projectVersionId}/vulnerable-bom-components API 请求中新增了一个可选的 showUnscoredRelatedVulnerability 参数。此参数接受 true/false 值，用于在 vulnerable-bom-components API 的响应中包含或排除未评分的相关漏洞。

如果不包含该参数或设置为 false，API 响应将与现有行为保持一致。当设置为 true 时，即使 BDSA 和 CVE 之间的影响组件版本范围不同，BDSA 也将始终列出相关的 CVE。这是为了帮助在下游漏洞处理流程中使用 CVE ID 的客户。

API 弃用通知

从 Black Duck 2024.7.1 版本开始，以下三个 API 已被标记为弃用，并将在即将发布的版本中移除：

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

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

二进制扫描程序信息

二进制扫描程序已更新为版本 2024.6.3。

已修复的问题

此版本中修复了以下客户报告的问题：

- (HUB-42054)。修复了以下问题：/api/projects/{projectId}/versions/{projectVersionId}/risk-profile API 请求因组件选项卡上忽略的已确认代码段匹配类型而返回未知安全风险。
- (HUB-42392)。修复了以下问题：在清除未映射的旧扫描时，可能出现 ERR05_1028 异常错误。
- (HUB-42549)。修复了以下问题：在 BOM 计算期间，会重复出现 LicenseConflictBaseStrategy 警告。
- (HUB-42626)。添加了针对以下问题的解决方法：在配置了 DNS 服务器的某些情况下，curl/c-ares 软件包（包含在所有基于 alpine 的映像中）中的一个错误会阻止 cfssl 域的解析，从而导致容器因无法获得部署所需的证书而崩溃。

  注意：c-ares 的维护者已发布了针对此错误的补丁。然而，它尚未在 Alpine Linux 的稳定版本中发布，并且发布时间表目前还不确定。
- (HUB-42786)。修复了以下代码段匹配查询优化问题：具有大量未确认代码段匹配的项目版本可能会导致 BOM 组件页面加载速度更慢。
- (HUB-42811)。修复了 vulnerable-bom-components 端点的 API 分页问题，该问题可能会影响存在大量漏洞（500 个以上）的项目。
- (HUB-42922)。修复了以下问题：在“受漏洞影响的项目”页面上，修改修复状态可能会失败，并在“更新修复计划”对话框中显示“无法读取未定义的属性（正在读取‘协议’）”错误。
- (HUB-42939)。修复了以下问题：IdP 元数据未刷新。 Black Duck 现在将每半小时重新加载一次 SAML 配置，其中包括 IdP 元数据。
- (HUB-43029)。修复了以下问题：使用非标准用户和组运行 Webapp 时，由于生成 zip 文件时出错，可能导致用户界面上无法显示日志文件。
- (HUB-43052)。修复了“扫描”页面上的以下排序问题：多次对“已更新”列进行排序，然后按另一列排序，导航离开再返回该页面而不刷新可能导致页面不保留“已更新”列的排序顺序。
- (HUB-43060)。修复了以下问题：尽管设置了换行符，但“设置”页面上的自定义字段详细信息仍未换行。
- (HUB-43257)。修复了以下问题：如果浏览器本地语言设置为不支持的语言，“新增功能”窗口中显示的内容将无法呈现。
- (HUB-43258)。修复了以下问题：在 source.csv 报告中，版本详细信息报告的“组件策略状态”和“由...覆盖”列为空。
- (HUB-43378)。修复了以下问题：--detect.code.location.name 参数不适用于 BDBA 扫描。

Black Duck SCA 2024.7.0

公告

KnowledgeBase 升级后的升级

请注意，KnowledgeBase 更新作业将在 Black Duck 升级完成后运行。此更新解决了由于之前的错误而导致的 KnowledgeBase 组件许可证数据过时的问题。根据部署的规模，该作业可能需要 4 个小时才能完成，但

通常的持续时间较短。此进程不会影响扫描或其他 Black Duck 进程。但是，在执行此作业期间，您可能会发现 Job runner pod 中的 CPU 和内存使用量增加。

更新活动审核跟踪

活动审核跟踪功能允许在影响项目和/或项目版本的应用程序中保留用户操作和关键事件的活动审核记录，比如项目版本组件和漏洞记录。

通过此次更新，现在可以禁用该功能，以提高性能并降低存储成本，让您更灵活地控制项目审核记录。禁用活动审核跟踪后，不会跟踪活动数据。重新启用后，将从那一刻起开始跟踪活动。

对于新的安装，此功能默认处于禁用状态，但对于现有安装和升级，此功能仍保持启用状态。

PostgreSQL 16 对外部数据库的支持

Black Duck 对于使用外部 PostgreSQL 的新安装，现在支持并建议使用 PostgreSQL 16。但是，Google CloudSQL for PostgreSQL 尚不支持 PostgreSQL 16；在该平台上，Black Duck 建议使用 PostgreSQL 15。

迁移到 2024.7.x 不需要迁移到 PostgreSQL 16。

内部 PostgreSQL 容器的用户无需执行任何操作。

即将终止对 PostgreSQL 14 的支持

随着 2024.10.0 版本即将发布，Black Duck 将结束对外部 PostgreSQL 14 的支持。请参阅 Black Duck 2023.10.0 版本。有关更多信息，请参阅 PostgreSQL 升级计划页面。

PostgreSQL 容器即将迁移到版本 15

Black Duck 将在 2024.10.0 版本中将其 PostgreSQL 映像迁移到版本 15。不使用 Black Duck 提供的 PostgreSQL 映像的客户不会受到影响。

即将针对 PostgreSQL 容器用户的升级限制

对于 Black Duck 提供的 PostgreSQL 容器的用户，Black Duck 2024.10.0 将仅支持从使用 PostgreSQL 版本 13 或 PG 14 容器的早期 Black Duck 版本直接升级（2022.10.0 至 2024.7.x（含））。

从旧的 Black Duck 版本（2022.10.0 之前）升级需要两步升级：

1. 升级到 Black Duck 2023.7.x。
2. 升级到 Black Duck 2024.10.x。

即将进行的 Web 服务器技术替换

在即将发布的 Black Duck 版本（2024.10.0 或 2025.1.0）中，现有的 ingress Web 服务器 (NGiNX) 将被新技术 Apache APISIX 所取代。现有自定义 NGiNX 配置的客户需要更新其设置，以确保兼容性。

文档本地化

2024.4.0 版本的 UI、联机帮助和发行说明已本地化为日语和简体中文。

从 2024.7.0 开始，更新的日语和简体中文本地化文档一经推出，将立即发布在 Black Duck 文档门户上。

新增和更改的功能

“新增功能”窗口

通过全新的“新增功能”窗口，了解 Black Duck 当前版本中引入的最新功能和增强功能。升级后，登录时即可显示“新增功能”窗口，突出显示此版本中最为重要的更新。

用户可以选择在以后登录时禁用此窗口，但此窗口将在下次 Black Duck 服务器升级时重新出现。即使在关闭后，也可以从帮助菜单的下方访问“新增功能”内容。从 2024.7 起，Black Duck 的所有主要版本都将包含“新增功能”内容。

新的长期支持 (LTS) 功能

长期支持 (LTS) 项目版本可以跟踪已发布产品版本的漏洞数据。LTS 项目适用于最终用户或客户已在使用的软件。LTS 项目在设计时即考虑到了可扩展性，可以支持极高数量的项目版本。

LTS 项目版本保留 Active 项目版本中的最少数据，重点跟踪 LTS 物料清单 (BOM) 内组件中新发现的漏洞。将 Active 版本转换为 LTS 时，会自动创建软件物料清单 (SBOM)，以便于与所需的第三方共享。虽然 LTS 版本目前不支持通知，但当新的漏洞数据发布到 Black Duck KnowledgeBase 时，这些版本将收到新的漏洞数据。

新的 BDSA AI Assisted 标签

我们引入了一种新机制，利用 AI 模型自动创建 BDSA，并推出了“AI Assisted”BDSA 标签。AI Assisted Security Advisory 由 Black Duck 的网络安全研究中心使用自动化 AI 工具自动创建。这些 BDSA 并未经过 BDSA 团队的独立验证，而是使用自动流程和生成式 AI 辅助创建的。这些公告旨在对我们的网络安全研究中心确定和验证的 BDSA 进行补充。

您会在发现其他漏洞标签的所有区域中找到 AI Assisted 标签：

- 作为“查找”页面上的漏洞过滤器
- 作为项目版本“安全”页面的过滤器
- 作为策略的漏洞条件

新的内部 SSL 证书到期警报

Black Duck 2024.7.0 引入了新的内部 SSL 证书到期警报。当用户的内部 SSL 证书即将到期时，该警报会提前 30 天通知用户，确保及时续订和不间断的安全连接。

新的 SBOM 保留配置

当客户生成要分发的 SBOM 时，SBOM 管理解决方案必须保留 SBOM，以便在需要时可以复制。这与其他类型的 Black Duck 报告不同，虽然它通常是发布流程的一部分，发生在预计不会对 BOM 进行进一步更改的时间点上，但情况并非总是如此。

使用此新功能，您现在可以为标准项目和 LTS 项目配置项目版本 SBOM 报告的保留期。

可以在“管理”→“系统设置”→“数据保留”→“SBOM 保留”中配置 SBOM 保留设置。

过滤 SBOM 模板中间接依赖关系的新选项

SBOM 模板现在有了一个选项，可在 SBOM 中只包含组件的直接依赖关系或无依赖关系的组件。该选项位于 SBOM 模板页面的“组件数据”部分的底部。默认状态为未选中，适用于 CycloneDX 和 SPDX 报告类型。如果未选中，则包含 BOM 中的所有组件。

注意：此信息可能仅适用于某些组件。

改进了报告中的版权处理

Black Duck 2024.7.0 对 SBOM 和通知文件报告中处理版权的方式进行了重大改进。变化包括：

- 增强了用于创建版权清单的算法。新算法将包括以前遗漏的版权，删除注释字符，并通过用真实字符替换转义字符代码使条目更具可读性。
- 版权列表现在按字母顺序排列，并删除了列表中的重复条目。
- 为通知文件报告提供更多自定义功能，包括排除许可证文本和许可证数据的功能。通知文件报告现在还包括一个部分，显示生成内容时使用的选定选项。
- 在“系统设置”中新增“版权”页面，允许您为 SBOM 和通知文件报告配置全局版权设置。选项包括合并日期不同的相同版权、删除不含日期的版权声明或使用标准版权标签。

改进了通知文件报告

通知文件报告得到了增强，增加了主页 URL 和更清晰的详细信息，适用于无版权的组件。从 2024.7.0 开始，没有版权的组件将显示 "No copyrights found"。

通过模糊匹配对无版本组件进行二进制匹配

二进制匹配在 Black Duck 中引入了新功能，用于通过二进制扫描识别组件版本。该技术利用新的 SaaS 匹配服务进行二进制扫描，当通过二进制分析未找到精确匹配时，会识别最接近的组件版本匹配。组件版本的匹配分数范围为 4（最低分数）到 100（最高分数）。

此更新还增加了对模糊匹配 API 的支持。使用模糊匹配组件版本的二进制匹配将显示各自的匹配分数以及找到的备选匹配数。该评分公式非常复杂，在不断改进 KnowledgeBase 的过程中，我们还将进一步改进匹配过程，并采用方法突出显示 BOM 上可能的最佳匹配。

更新了二进制扫描的最大尺寸

我们已将可扫描的二进制文件的最大尺寸从 5GB 增加到了 20GB。此更改解决了 Black Duck 托管环境中的安全限制问题，确保我们在支持扫描较大二进制文件的同时，维持稳健的安全性。

更新了扫描 BOM 导入日志

我们优化了 BOM 导入日志，以提高性能并降低存储成本：

- BOM 导入日志中将不再记录许可证丢失、未找到或已映射的记录。
- 仅保留最近的 BOM 导入日志。

这些改进简化了日志记录过程，并专注于最相关的数据，确保更有效地利用资源。

更新了项目创建过程

项目创建过程更新如下：

- 如果您的服务器上未启用 SCM 集成，单击“创建项目”按钮可直接进入创建项目表单。这种情况没有改变。
- 如果启用了 SCM 集成，单击“创建项目”按钮现在将显示一个下拉列表，其中包含“标准项目”和“SCM 项目”选项。单击“标准项目”，用户将进入创建项目表单。单击“SCM 项目”，用户将进入 SCM 服务器选择页面。

更新了报告视图中的 component_vulnerability 表

component_vulnerability 表新增了 remediation_updated_at 字段。该字段记录了上次更新漏洞分类状态的日期。

二进制扫描迁移到 protobuf 格式

传统的 jsonid 二进制扫描已迁移到 2023.10.0 中引入的 protobuf 格式，适用于所有使用 BDBA 的扫描。此次迁移无需更新环境，扫描结果也不会受到影响。

项目设置和组件中新增了 SBOM 字段

新增了以下 SBOM 字段：

- 发起者：项目、BOM 组件
- 下载位置：组件版本、自定义组件版本

增加了对 Signature Scanner 的 macOS ARM64 支持

Signature Scanner 现在支持 macOS ARM64。此更新确保 Black Duck 产品之间的兼容性，为基于 ARM64 的系统提供更高的性能和无缝操作。

删除了指定策略规则条件的 "IN" 运算符

以下策略规则条件不再允许使用 "IN" 运算符。此更改仅适用于新的和更新的策略规则。现有策略不受影响。

- 新版本计数
- 严重严重性漏洞计数
- 高严重性漏洞计数
- 中等严重性漏洞计数
- 低严重性漏洞计数

支持的浏览器版本

- Safari 版本 17.5
  - 不再支持 Safari 版本 14 和更低版本
- Chrome 版本 126.0.6478.127（正式版本）(x86_64)
  - 不再支持 Chrome 版本 91 和更低版本
- Firefox 版本 128.0（64 位）
  - 不再支持 Firefox 版本 89 和更低版本
- Microsoft Edge 版本 123.0.2420.97（正式版本）（64 位）
  - 不再支持 Microsoft Edge 版本 91 和更低版本

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

删除弃用的匹配组件 API 请求

以下弃用的 API 请求已在 2024.7.0 版本中删除：

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

新的 vulnerable-bom-components 版本

添加了以下 API 请求的新版本 (V8)：

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

该 API 请求的最新版本改进了性能，并进行了以下修复，以提高输出质量：

- 在新的轻量级版本中，vulnerabilityName 字段已从 /api/projects/<project-id>/versions/<version-id>/vulnerable-bom-components API 请求中删除，因为 vulnerabilityName 和 vulnerabilityId 字段具有相同的值，而且 vulnerabilityId 更常用。

二进制扫描程序信息

二进制扫描程序已更新为版本 2024.6.2。

已修复的问题

此版本中修复了以下客户报告的问题：

- (HUB-34550)。修复了基于 Web 浏览器区域设置的短数字日期的显示方式。例如，欧洲区域设置现在显示日/月/年日期格式。
- (HUB-40168)。修复了版权显示问题。有关详细信息，请参阅 改进了报告中的版权处理。
- (HUB-40687)。修复了“查找”页面上未正确显示上次扫描时间的问题。
- (HUB-40774)。修复了以下问题：CVSS 3 攻击向量值为“邻近网络”的漏洞之前已映射到 Black Duck 且值为空。从 2024.7.0 起，该值已正确映射，并将触发一次性作业，为任何 CVSS 3 攻击向量字段为空的缓存漏洞填写该数据。

- (HUB-41220)。修复了在“查找”页面上搜索漏洞时可能显示错误严重级别的问题。
- (HUB-41264)。修复了以下问题：扫描页面（具有代码段匹配）与单击“导出当前视图”按钮时生成的 .CSV 文件显示的扫描大小不一致。
- (HUB-41348)。修复了“扫描”页面上的一个问题：在包含代码段时，按大小排序的扫描不正确。
- (HUB-41683)。在新的轻量级版本中，vulnerabilityName 字段已从 /api/projects/<project-id>/versions/<version-id>/vulnerable-bom-components API 请求中删除，因为 vulnerabilityName 和 vulnerabilityId 字段具有相同的值，而且 vulnerabilityId 更常用。
- (HUB-41851)。将版本详细信息报告（项目版本升级指南）中重复的 "Component Origin Id" 列重命名为组件来源外部 ID。
- (HUB-42041)。修复了以下问题：一旦在全局级别对组件的详细信息设置/许可证/自定义字段进行了编辑，并尝试返回到 Black Duck 中之前访问过的页面时，就会丢失导航，并且永远无法返回。
- (HUB-42054)。修复了以下问题：/api/projects/{projectId}/versions/{projectVersionId}/risk-profile API 请求因组件选项卡上忽略的已确认代码段匹配类型而返回未知安全风险。
- (HUB-42155)。修复了以下问题：项目版本自动删除的上次更新时间戳被系统计算和其他项目调整错误修改。
- (HUB-42225)。修正了项目版本“来源”选项卡上的一个问题：“不匹配”过滤器选项同时显示不匹配的文件和不匹配的组件，导致难以在结果中找到不匹配的组件。该过滤器现在拆分为两个单独的值：不匹配的文件（仅显示不匹配的文件）和不匹配的 ID（仅显示不匹配的组件 ID）。
- (HUB-42260)。修复了以下问题：在某些情况下，UI 和漏洞报告中 CVE 漏洞的利用状态可能不一致。
- (HUB-42363)。修复了以下问题：直接/间接访问项目的用户无法查看容器扫描的图层信息。
- （HUB-42402、HUB-42471）。修复了以下问题：没有映射扫描的项目版本未被安排为项目版本自动删除。
- (HUB-42466)。修复了以下问题：使用软件包管理器扫描大型项目时，输出文件中可能包含超过 10,000 个图形节点，从而可能导致扫描容器最终超时。
- (HUB-42478)。修复了以下问题：在使用 hub_db_migrate.sh 时，由于在报告数据库 matviews 的定义中没有正确传递 search_path，导致报告数据库无法填充。
- (HUB-42531)。修复了以下问题：在使用只读 YAML 文件进行部署时，尝试下载系统日志可能会生成“未找到日志文件”错误。
- (HUB-42545)。修复了以下问题：长期支持 (LTS) 项目不会显示在向项目版本添加项目的模式中，而且在手动调用 API 时，也未显示在组件列表中。
- (HUB-42753)。修复了以下问题：二进制匹配会错误地在 API 为 BOM 匹配设置的计数中添加额外的 ID。这种差异影响了匹配置信度，导致其与模糊匹配中的备选项数量不一致。
- (HUB-42760)。修复了以下问题：在创建添加了组件类别的版本详细信息报告时，缺少“代码段审查状态”列。
- (HUB-42811)。修复了一个分页问题：无论值设置为什么，vulnerable-bom-components API 端点的 offset 值都会返回相同的结果。
- (HUB-42873)。修复了以下问题：SBOM 版权报告可能会因无法验证 BOM 中是否存在组件而失败。
- (HUB-42953)。修复了以下问题：版本详细信息报告中的风险概况错误地使用了运维风险中等计数，而不是许可证中等风险计数。
- (HUB-43001)。修复了有关自动扫描重试标头配置的文档的问题。

Black Duck SCA 2024.4.x

Black Duck SCA 2024.4.1

公告

即将合并 OpenShift/Kubernetes 文档

随着 2024.7.0 版本的发布，我们将对 OpenShift 的支持过渡到基于 Kubernetes helm 的部署。当前的 OpenShift 独立安装指南将停止使用，并合并到 Kubernetes 安装指南中，其中的一些章节是为 OpenShift 量身定制的。

Black Duck 将继续在 OpenShift 环境中受支持，但需要使用我们的 Kubernetes helm 图表配置来安装和升级。请参阅我们的安装文档或联系 Black Duck 支持人员以获得更多指导。

新增和更改的功能

改进 BOM 导入日志

BOM 导入日志现在会将 SBOM 导入中任何没有 PURL 的不匹配组件添加到 BOM 导入日志中，使其可见且可操作。错误消息现在清楚地指出了特定组件无法匹配的原因：

- 如果 PURL 在 KnowledgeBase 中没有匹配项，则显示的错误消息为 Unable to map scanned component version to Black Duck project version because no mapping is present for the given external identifier。
- 如果 PURL 无效，则显示的错误消息为 Unable to map scanned component version to Black Duck project version because given external identifier is invalid。
- 如果 PURL 缺失，则显示错误消息为 Unable to map scanned component version to Black Duck project version because no external identifier is provided。

改进了 ReversingLabs 扫描结果

Black Duck 2024.4.1 包括对 ReversingLabs 恶意软件扫描的增强。现在，所有恶意软件扫描都将包括具体的恶意软件威胁名称，为您提供有关检测到的威胁的更详细、更精确的信息，旨在提高您更有效地应对安全问题的能力。

请注意，要利用此新更新，必须重新运行 ReversingLabs 扫描，才能在扫描结果中看到新的威胁名称。

容器版本

- 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 增强

Black Duck 2024.4.1 中没有新增或更改的 API 请求。有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

二进制扫描程序信息

2024.4.1 中的二进制扫描程序没有更改。

已修复的问题

在此发布中修复了客户报告的以下问题：

- (HUB-39354)。修复了以下问题：软件材料清单 (SBOM) 中的项目别名字段只能覆盖项目级别的主项目名称和版本，而不会扩展到 SBOM 报告中的子项目。
- (HUB-39807)。修复了以下问题：UI 中的 vulnerable-bom-components API 端点可能无限期挂起。
- (HUB-41575)。修复了以下问题：从扫描列表下载存档文件时，下载的文件类型错误，导致以 BDIO 文件上传时出现错误。
- (HUB-41670)。修复了以下问题：scan pod 访问 rabbitmq admin 插件时遇到问题，无法在启用了速率限制的托管环境中进行重试。
- (HUB-41753)。修复了以下问题：SPDX SBOM 报告导出中缺少 DESCRIBES 关系。
- (HUB-41992)。修复了以下问题：在为自定义字段创建策略时，包含 "/" 字符的自定义字段可能会导致条件列表空白。
- (HUB-42086)。修复了以下问题：api/versions/<versionID>/reports 端点在 API 输出的 riskProfile 部分中显示的信息不清楚。
- (HUB-42101)。修复了以下问题：在处理没有 cvss3 分数的条目时，VULNERABILITY_REPRIORITIZATION 作业可能会卡住。
- (HUB-42158)。修复了以下问题：SBOM SPDX 报告未显示“SSLeay 许可证 — 独立”的正确许可证名称。
- (HUB-42208)。修复了以下问题：某些实例的“作业”页面上缺少错误状态过滤器。
- (HUB-42304)。为 st.version_bom_entry(code_location_id) 表添加了一个索引，来帮助减轻特定表的压力。
- (HUB-42334)。修复了项目版本页面的“恶意软件”选项卡上的排序顺序问题，该问题可能导致规则 ID 条目重复。
- (HUB-42382)。修复了以下问题：在文件树中取消选择匹配项后，“来源”选项卡未重新显示匹配项。

- (HUB-42585)。修复了以下问题：新的 SAML 和 LDAP 用户帐户添加到指定默认用户组时，无法正确进行身份验证。

Black Duck SCA 2024.4.0

公告

更新操作系统支持

安装 Black Duck 2024.4.0 的首选操作系统已更新如下：

- 终止对 CentOS 7 的支持。
- 终止对 Red Hat Enterprise Linux 服务器 7.9 和 8.6 的支持。
- 增加对 Red Hat Enterprise Linux 服务器 8.9 和 9.x 的支持。

弃用并即将移除允许/拒绝 nginx 配置

Black Duck 2024.4.0 已弃用 blackduck-nginx 内置的以下功能：

- DENY_ACCESS_DIRECTIVES
- ALLOW_ACCESS_DIRECTIVES

这些功能将在 Black Duck 2024.7.0 中完全移除。

文档本地化

2024.1.0 版本的 UI、联机帮助和发行说明已本地化为日语和简体中文。

新增和更改的功能

针对 PostgreSQL 16 的初步支持

Black Duck 2024.4.0 增加了对使用 PostgreSQL 16 作为外部数据库的初步支持。此支持仅用于测试；不支持生产用途。

新的 ReversingLabs 恶意软件扫描

ReversingLabs 扫描允许您通过我们与 ReversingLabs 的合作伙伴关系访问增强型恶意软件和威胁情报数据。利用由 ReversingLabs 提供的复杂二进制分析功能，开发人员和 DevOps 团队可以分析第一方、开源和商业软件，以识别是否存在恶意软件、恶意代码、可疑文件、潜在有害应用程序 (PUA)、抗议软件和可疑文件结构畸形等威胁，从而帮助避免危险的软件供应链攻击。

新的不匹配的组件自动创建

在 SBOM 管理工作流中，SBOM 是输入，SBOM 中包含的所有组件都需要持久保存在 SBOM 管理解决方案中，这样无论是否与 KnowledgeBase 匹配，都不会丢失可见性。此功能提供了一个选项，即只要组件在 SBOM 中具有关联的 PURL，就可以在 BOM 表中自动创建与 SBOM 导入中同名的自定义组件不匹配的组件。

此外，在 SBOM 许可证标签值为 NOASSERTION 时，您还可以配置应用于自动创建组件的默认许可证。

新的 SBOM 模板

SBOM 模板是一项新功能，可有效取代并增强确定 SBOM 报告中内容的能力。SBOM 模板允许用户选择要在生成的 SBOM 中包含哪些字段，以及其他一些配置项，比如是否包含漏洞信息（针对 CycloneDX）或开发/构建工具。然后，在创建 SBOM 报告时，可以选择 SBOM 模板以生成所需的输出。

请注意，一些 SBOM 字段配置已从项目组设置移至 SBOM 模板配置。我们鼓励客户在升级到 Black Duck 2024.4.0 之后，在生成新的 SBOM 报告之前查看和配置 SBOM 模板。

为项目组添加了新的 CLI 命令行选项

您现在可以将 --project-group 选项添加到特征扫描命令行中，该命令行设置要将项目分配到的“项目组”。如果项目不存在，则会在相应的项目组中创建一个新项目。

如果项目已存在，或指定的项目组不存在，则此参数无效。

增加了对 CycloneDX 1.5 的支持

您现在可以用 CycloneDX v1.5 格式导出项目的软件材料清单报告。这可以通过查看项目版本，单击“报告”选项卡，单击“创建报告”按钮，然后选择 CycloneDX v1.5 — JSON 来完成。有关 CycloneDX v1.5 的更多信息，请访问 CycloneDX v1.5 参考页面。

增强了丢失容器扫描注册错误处理

如果 Black Duck 注册密钥未启用容器扫描，容器扫描现在将失败并显示相应消息。

增强了 SBOM 导入错误处理

改进了 SBOM 导入错误处理，以便更好地了解 SBOM 导入失败的原因，包括未能通过验证的具体行/字段。此外，您还可以将故障导出到日志文件，以便在 Black Duck UI 之外进行研究，并在对 SBOM 进行必要的更新后尝试重新导入。

更新了设置 HUB_MAX_MEMORY 的方法

从 Black Duck 2024.4.0 开始，在基于 Kubernetes 的部署中，会自动为相关容器设置配置参数 HUB_MAX_MEMORY。该值按内存限制的百分比计算，默认值为 90%。在 gen04 部署调整中，hubMaxMemory 设置已替换为 maxRamPercentage 来控制使用的百分比；选择此设置的值，以使 HUB_MAX_MEMORY 具有与之前相同的值。

此更改不适用于基于 Swarm 的部署。

更新了通过 SBOM 导入的组件的匹配分数置信度

在查看从 SBOM 文件导入组件的项目版本 BOM 时，显示的匹配分数始终为 100%，且匹配类型显示 SBOM 为来源。

更新了 BDBA 软件包管理器支持的二进制匹配类型结果

以前，所有容器和二进制扫描都会生成单个二进制匹配类型。随着 BDBA 软件包管理器支持范围的扩大，我们现在可以根据 BDBA 匹配方法识别更多的匹配类型。因此，您将看到 BOM 中的变化，通过二进制和容器扫描识别的组件将获得或改变其匹配类型。

删除 blackduck-webui 容器

blackduck-webui 容器已被删除，其构建现在包含在 blackduck-nginx 容器中。blackduck-nginx 容器现在将遵循与 blackduck 堆栈的其余部分相同的发布节奏。

支持的浏览器版本

- Safari 版本 17.4.1
  - 不再支持 Safari 版本 14 和更低版本
- Chrome 版本 123.0.6312.124（正式版本）(x86_64)
  - 不再支持 Chrome 版本 91 和更低版本
- Firefox 版本 124.0.2（64 位）
  - 不再支持 Firefox 版本 89 和更低版本
- Microsoft Edge 版本 123.0.2420.97（正式版本）（64 位）
  - 不再支持 Microsoft Edge 版本 91 和更低版本

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

SBOM 创建者和 SBOM 名称字段的新组件过滤键

以下 API 请求添加了新的过滤键，可返回 BOM 组件的 SBOM 名称和创建者的可能值：

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

过滤键：

- sbomName
- sbomCreator

对 SBOM 创建者和 SBOM 名称字段的新组件过滤支持

为以下 API 请求添加了新的过滤器：

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

过滤器：

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

匹配 REST API 请求的新代码段（生成式 AI 合规）

添加了以下 API 请求，允许您查找给定代码段的匹配项：

- POST /api/snippet-matching

这些匹配项按许可证系列排序，以更好地显示特定匹配项所代表的风险（PERMISSIVE、WEAK_RECIPROCAL、RECIPROCAL、RECIPROCAL_AGPL、RECIPROCAL_NETWORK、UNKNOWN）。

弃用匹配的组件 API 请求

以下匹配的组件 API 请求已被弃用，并将在 Black Duck 2024.7.0 中删除：

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

二进制扫描程序信息

二进制扫描程序已更新为版本 2024.3.0。

已修复的问题

在此发布中修复了客户报告的以下问题：

- (HUB-39206)。修复了以下问题：二进制扫描程序无法检测到 .DEB 文件组件，导致这些组件无法显示在结果报告中。
- (HUB-39395)。修复了以下问题：KnowledgeBase 更新将上次更新的用户显示为在组件管理中添加组件的用户。由 KnowledgeBase 更新作业更新的自定义组件现在将显示为系统用户。
- (HUB-39635)。修复了以下问题：当 Detect CONTAINER_SCAN 与其他扫描类型（例如 DETECTOR 或 BINARY _ SCAN）一起运行时，Detect 未返回预期的 412 Precondition Failed 错误消息。
- (HUB-40531)。修复了以下问题：组件报告可能为某些组件生成重复条目。
- (HUB-40745)。修复了一个 SPDX SBOM 报告问题：当 BOM 中同一组件版本有多个来源时，PackageSupplier 字段可能与 Purl 字段中的来源名称不同。
- (HUB-40769)。弃用了 API 请求 GET /api/projects/{projectId}/versions/{projectVersionId}/matched-components，因为它在使用时返回 404 错误。
- (HUB-40870)。修复了以下问题：在构造 URL 编码时，对指向组件版权页面的 "origins-with-filters" 链接的搜索参数进行编码。
- (HUB-40930)。修复了本地化 CSV 文件中的一个问题：在 Excel 中打开搜索结果时会显示乱码字符。
- (HUB-40998)。修复了以下问题：当用户删除 SBOM 报告中的“软件包有效截止日期”字段时，该字段未清除。
- (HUB-41041)。修复了 SCAaaS helm 图表自述文件中的一个链接断开。

- (HUB-41063)。修复了以下问题：如果“过渡”和“直接”匹配都存在于同一组件版本中，则只会显示“直接依赖关系”。
- (HUB-41132)。修复了以下问题：搜索包含 + 特殊字符的组件时无法返回预期结果。
- (HUB-41167)。修复了有关列出项目版本 API 支持的过滤器的 REST API 文档。唯一支持的过滤器是阶段、许可证和发行版。
- (HUB-41276)。修复了以下问题：具有未知许可证的组件不会包含在通知文件报告中。
- (HUB-41299)。修复了以下问题：以前映射后删除的自定义组件会被错误地重新映射，从而影响后续扫描中未匹配组件的总数。
- (HUB-41316)。修复了以下问题：将 SaaS 升级到 2023.7.3 时可能导致 SSO 失败。
- (HUB-41318)。修复了搜索组件版本时行为不一致的问题。
- (HUB-41321)。修复了以下问题：.ZIP 文件中的代码段结果注释未导出到源报告。
- (HUB-41362)。修复了以下问题：发现过滤器显示所有发现，而不是基于在搜索字段中输入的文本的搜索结果。
- (HUB-41365)。修复了以下问题：当 /api/projects 限制设置为 0 (/api/projects?limit=0) 时可能导致无法加载结果页面。
- (HUB-41369)。修复了以下问题：上传的品牌标识不会自动缩小，以符合预期的尺寸要求。
- (HUB-41391)。修复了以下问题：SBOM 中格式错误的 PURL 字段可能导致 CycloneDX 无法导入 SBOM 文件。
- (HUB-41431)。修复了有关项目经理角色和项目删除权限的文档问题。
- (HUB-41450)。更新了自述文件，在部署命令中的 sizing.yaml 之前正确排序 values.yaml 文件。
- (HUB-41461)。修复了以下问题：使用列出受影响的项目版本 API 时显示的总数是项目数，而不是项目版本数的问题。
- (HUB-41502)。解决了在 SCAaaS 部署中发现的安全问题。
- (HUB-41542)。修复了以下问题：在模糊 BDBA 扫描时，kbupdatejob 组件更新会重置 BOM 上次更新日期。
- (HUB-41549)。修复了以 CSV 格式导出用户列表时的本地化问题。
- (HUB-41552)。修复了在禁用项目版本自动删除功能并重新启动系统时，无论数据保留策略如何，该功能与保留项目版本交互的问题。
- (HUB-41570)。修复了以下问题：scan_stats_view 具体化视图需要很长时间才能执行。
- (HUB-41591)。修复了 HUB CloudSQL 数据库中由删除查询引起的死锁问题。
- (HUB-41773)。修复了尝试上传文件夹中的多个文件，并将它们拖到上传 SBOM-SPDX 文件或上传 SBOM-CycloneDX 文件时出现的问题。
- (HUB-41867)。修复了以下问题：由 KB 更新作业和 BOM 软件包调整（用户手动将 BOM 中不匹配的外部 ID 映射到 KB 组件）生成的任何漏洞通知具有不正确的“未知”事件源。
- (HUB-41930)。修复了以下问题：除非运行 pod 的用户是 root (0) 或 nginx (101)，否则 nginx Web 服务器将无法启动。
- (HUB-41974)。修复了“项目版本”->“来源”选项卡上的不匹配过滤器显示错误计数的问题。
- (HUB-42004)。修复了以下问题：在 SSO 登录后立即访问 Black Duck 中的页面时，用户无法进入预期页面。
- (HUB-42051)。修复了以下问题：清除 UI 中的组件下载位置时，version_bom_component 中的 download_location 值未被移除。

Black Duck SCA 2024.1.x

Black Duck 2024.1.1

公告

Black Duck 2024.1.0 Job runner 问题 (HUB-41654)

2024.1.0 中发现了一个严重的错误 (HUB-41654)，它影响到 Black Duck Job runner 和 KnowledgeBase 更新检查作业。此错误导致更新 KnowledgeBase 数据作业无法将更新应用到存在新漏洞或已修改漏洞的 BOM。这个问题只有在特定的漏洞条件下才会出现，而且可能只影响少数客户 BOM。我们建议运行 2024.1.0 的客户尽快升级到 2024.1.1 以解决此问题。

此问题仅影响运行 2024.1.0 的客户。有关更多详细信息，请参阅有关此问题的社区公告。

新增和更改的功能

新的“项目版本 SBOM”字段配置

现在，当组件用作项目版本的子项目时，您可以配置项目版本 SBOM 字段来定义 BOM 组件 SBOM 字段，以便在 SBOM 中提供适当的详细级别，而不必为子项目中使用的每个项目定义。

更新了搜索功能

用于在 Black Duck 中搜索的算法已得到增强，并将扩大搜索范围，通过检索包含字符串或部分匹配的所有记录，让您更轻松地找到所需的信息。它将提供与使用 Solr 搜索类似的结果，即使不知道完整的字符串，也能找到相关记录。

容器版本

- 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 增强

更新了项目版本策略规则摘要 API

添加了新版本的项目版本策略规则摘要 API，它提供了策略规则违规及其关联 BOM 组件计数的分页列表：

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

以前的版本已被弃用，并将在即将发布的 Black Duck 版本中删除。

更新了 BOM 漏洞端点

添加了易受攻击的 BOM 组件端点的新版本 (V8)，其中包含性能改进：

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

版本 8 的端点仅包含为当前 UI/UX 视图或自定义集成实用程序提供服务所需的最低数据量，以便更快地产生结果并防止超时失败。请注意，此 API 端点的 V7 版本也已发布，并映射到现有的 V6。

二进制扫描程序信息

Black Duck 2024.1.1 中的二进制扫描程序没有更改。

已修复的问题

在此发布中修复了客户报告的以下问题：

- (HUB-38966)。修复了以下问题：由于涉及策略表达式为较新版本计数的风险数据缺失，策略评估可能会失败。
- (HUB-40443)。修复了 UI 和报告之间的策略违规差异的聚合器功能问题。
- (HUB-40666)。修复了以下问题：KbUpdate 许可证作业完成后许可证分配可能不会更新。
- (HUB-40690)。修复了 rabbitmq 更新引起的问题，该问题可能会导致 Kubernetes 出现虚假故障错误。
- (HUB-40861)。修复了以下问题：在 Black Duck 中搜索带有“破折号”和空格的组件时，除非双倍行距，否则不会返回结果。
- (HUB-40975)。修复了以下问题：尝试批量编辑不匹配的组件可能会生成错误消息（应用程序遇到未知错误）。
- (HUB-41054)。修复了以下问题：项目版本的源报告可能会输出重复的条目。
- (HUB-41069)。修复了以下问题：CycloneDX SBOM 报告中不存在供应商字段。
- (HUB-41281)。修复了以下问题：单击 BOM 报告中的“打印”按钮时组件被截断。
- (HUB-41295)。修复了以下问题：以非系统管理员用户身份登录时，“创建自定义字段”页面上缺少“创建”按钮。
- (HUB-41347)。修复了以下问题：当全局设置被禁用时，特定版本的扫描保留设置仍可用。
- (HUB-41390)。修复了以下问题：当 /api/internal/dashboard-facts API 请求使用过多参数时，可能会发生错误。

- (HUB-41396)。修复了导致更新 KnowledgeBase 数据作业无法将更新应用到存在新漏洞或已修改漏洞的 BOM 的问题。有关更多信息，请参阅相关公告。
- (HUB-41463)。修复了以下问题：无法从系统日志中捕获 BDBA 工作日志。
- (HUB-41502)。更新了以下 SCAaaS 组件版本以解决安全漏洞：

组件名称	以前的版本	新版本
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
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

公告

移除上传缓存服务

加密现在由 Black Duck 密钥加密库和密钥轮换机制处理。因此，用于处理 SEAL_KEY 更改的 recover_master_key.sh 和 bd_get_source_upload_master_key.sh 脚本已经移除。

同样，不会迁移 Black Duck “来源” 选项卡使用的上传的源文件。如有需要，您可以在现有或新的临时项目中重新扫描来源。请注意：来源上传仍必须使用 ENABLE_SOURCE_UPLOADS（默认为 false）显式启用，并且仍会自动删除，从而满足 MAX_TOTAL_SOURCE_SIZE_MB（默认为 4G）与 DATA_RETENTION_IN_DAYS（默认为 180 天）的配置设置要求。

注意：上传的源代码默认不会迁移，迁移脚本不包含在 Black Duck 2024.1.0 版本中。如果您需要在升级期间迁移上传的源代码，请联系 Black Duck 支持人员。

扫描硬件要求变化

Black Duck 2024.1.0 扫描硬件要求将发生一些变化，因此 Black Duck 客户需要更新其环境，并在必要时根据以下指南分配额外的硬件资源。

请参阅 Black Duck 硬件扩展指南，了解更多信息。

表 1: 硬件扩展指南

名称	详细信息	
120sph	扫描次数/小时：120 SPH 百分比增加：0% API/小时：3,000 项目版本：13,000	IOPS：读取：15,000/写入：15,000 Black Duck 服务：CPU：11 核/内存：56GB PostgreSQL：CPU：4 核/内存：16 GB 总数：CPU：15 核/内存：72 GB
250sph	扫描次数/小时：300 SPH 百分比增加：20% API/小时：7,500 项目版本：15,000	IOPS：读取：15,000/写入：15,000 Black Duck 服务：CPU：16 核/内存：86 GB PostgreSQL：CPU：6 核/内存：24 GB 总数：CPU：22 核/内存：110 GB
500sph	扫描次数/小时：650 SPH 百分比增加：30% API/小时：18,000 项目版本：18,000	IOPS：读取：25,000/写入：25,000 Black Duck 服务：CPU：23 核/内存：133GB PostgreSQL：CPU：16 核/内存：64GB 总数：CPU：39 核/内存：197GB
1000sph	扫描次数/小时：1400 SPH 百分比增加：40% API/小时：26,000 项目版本：25,000	IOPS：读取：25,000/写入：25,000 Black Duck 服务：CPU：46 核/内存：367GB PostgreSQL：CPU：22 核/内存：88GB 总数：CPU：68 核/内存：455GB
1500sph	扫描次数/小时：1600 SPH 百分比增加：6% API/小时：41,000 项目版本：28,000	IOPS：读取：25,000/写入：25,000 Black Duck 服务：CPU：57 核/内存：459 GB PostgreSQL：CPU：26 核/内存：104 GB 总数：CPU：80 核/内存：563 GB
2000sph	扫描次数/小时：2300 SPH 百分比增加：15% API/小时：50,000 项目版本：35,000	IOPS：读取：30,000/写入：30,000 Black Duck 服务：CPU：64 核/内存：565GB PostgreSQL：CPU：32 核/内存：128GB 总数：CPU：96 核/内存：693GB

文档本地化

2023.10.0 版本的 UI、联机帮助和发行说明已本地化为日语和简体中文。

新增和更改的功能

新的 Black Duck Automated Security Advisory (ASA)

Automated Security Advisory (ASA) 由 Black Duck 的网络安全研究中心使用自动化 AI 工具自动创建。ASA 的创建基于各种可信的安全信息源（如 GitHub Security Advisories (GHSA) 信息源），并使用 AI 工具进行自动审核。这些公告旨在对我们的网络安全研究中心确定和验证的 BDSA 进行补充。

您会在发现其他漏洞标记的所有区域发现带有 ASA 标记的 BDSA。

BOM 组件的新下载位置值

新下载位置 SBOM 字段已经添加到附加字段列表。下载位置位于 BOM 组件部分的下方，可对其进行配置，您可以添加下载组件的版本控制系统 (VCS) 中的 URL 或其他特定位置。此新信息在 SBOM 报告中显示为：

- SPDX：在 packages > package ID 部分，显示为 downloadLocation。
- CycloneDX：在 components > externalReferences 部分，显示为 url。

SBOM 报告的新版权文本、许可证注释和主页数据

更新了项目组设置下的可用 SBOM 报告选项，以支持将版权数据、许可证注释和主页 URL 加入 SBOM 报告。如果组设置已启用，则 CycloneDX 和 SPDX 报告均可涵盖版权文本、许可证注释和主页 URL。

新的 SCM 存储库自动扫描

SCM 存储库自动扫描允许 Black Duck 每天检查映射到 SCM 项目的存储库分支中的任何更改（如提交、推送或合并），并在发生更改时执行扫描。如要利用这一功能，则必须启用该功能，启用方法是“管理 → 作业 → 已计划”。

此外，已经在 Black Duck 中添加了两个新的 SCM 存储库自动扫描作业以支持此功能：

- SCM Onboarding 每日自动扫描：安排夜间作业，自动执行扫描之前加入的 SCM 存储库。
- SCM Onboarding 每日清理：安排夜间清理 SCM Onboarding 的作业。

已添加 CISA 已知可利用漏洞标记

Black Duck 中现在会标记列于 CISA 已知可利用漏洞目录的漏洞。您由此可以添加 CISA 已知漏洞作为漏洞条件策略过滤器。请访问 CISA 已知可利用漏洞目录页面，了解更多信息。

SCM 集成更新

Black Duck 2024.1.0 在 SCM 集成列表中添加了两个新的 SCM 提供商：

- GitLab SaaS
- Bitbucket

现在，您可以添加这些授权的 SCM 提供商，然后在创建新项目时选择这些提供商。这样做之后，将自动在新项目的“项目设置”页面中预填充存储库 URL 和分支版本。

此功能与 Detect 8.x 及更高版本兼容，并将在新的软件包管理器扫描中生效。

请注意，在 Black Duck 中默认情况下不启用 SCM 集成，必须通过在您的环境中添加以下内容来激活此功能：

对于 Swarm 用户，请将以下内容添加到您的 blackduck-config.env 文件中：

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

对于 Kubernetes 用户，请将以下内容添加到您的 values.yaml 文件中的 environs 部分下：

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

SBOM 报告关系信息更新

更新了 SBOM 报告，以便添加依赖关系信息。目前 SPDX 报告的依赖关系包含 relationships 部分中的依赖关系类型。请注意：这仅适用于 SPDX 2.3 报告。CycloneDX 报告不包含依赖关系类型。

组件代码段匹配的深度许可证数据管理更新

利用深度许可数据 (DLD) 和代码段匹配的客户现在可以对其项目进行配置，从而查看在其代码中发现的存在于组件文件中的深度许可风险。

此功能已经被分解为两个独立的功能：

- 将深度许可证数据应用于材料清单：启用该复选框将对非代码段组件应用深度许可证数据，并允许查看组件中可能存在的嵌入式许可证（超出已声明的许可证）。

- 将深度许可证数据应用于组件代码段匹配：如果启用，则会在深度许可证数据计算中涵盖组件代码段匹配。

改善项目层次结构的许可证冲突管理

此前，许可证冲突仅根据单个项目许可证计算，而不会考虑项目层次结构。在 Black Duck 2024.1.0 中，父项目中的子项目现在也会纳入计算之中。

Black Duck 2024.1.0 默认启用分层许可冲突，但也可在环境中进行配置。不过，许可证冲突信息不会自动启用。系统管理员必须启用“法律和许可证冲突”选项卡，以便查看许可证冲突。使用项目的“设置”选项卡为当前项目启用该功能。

改善组件漏洞历史记录图表

显示在组件页面的漏洞历史记录图表现在会涵盖未知来源漏洞的数据。

改善适用于 SCA 的 Kubernetes 探针

对 Kubernetes 环境所使用的就绪探针做出改进：

- 已经添加新的 startupProbe，验证容器中的应用程序是否已启动。startupProbe 会在任何其他探针之前运行，且除非成功完成，否则会禁用其他探针。
- 现在，readinessProbe 会在初始延迟 30 秒后（原为 240 秒）开始检查，并每 10 秒检查一次（原为 30 秒）。在发出重启指令前，允许有 15 次故障机会。
- livenessProbes 现在每 10 秒检查一次（原为 30 秒）。
- 已经为 startupProbe 和 readinessProbes 添加新的开关。已经添加控制各探针的唯一标志。

改善按需作业重试

按需作业此前会尝试重试三次才最终失败，这在某些情况下会导致已知失败的作业继续重新运行，进而消耗系统资源。通过在默认情况下禁用重试，我们对这种方法进行了改进，这样当相应的检查作业再次运行时，会重试定期调度程序启动的作业。

请注意：此项更改不会影响报告作业。报告作业会正常重试。

对上传缓存进行更改以便进行源代码上传

注意：此项更改是 Black Duck 2023.10.0 的一部分，当时并未明确传达这点。

在 Black Duck 2023.4.2 中，为在 AWS 上运行的用户添加了一个解决方法，以处理上传源文件和使用许可证搜索功能无法工作的问题，原因在于文件系统延迟和生成多个 du 进程。

Black Duck 2023.10.0 对 Black Duck 使用上传缓存和存储服务的方式进行了架构更改，从而解决了这一问题。Black Duck 的源代码上传功能不再使用上传缓存，因此通过存储服务上传源代码的新架构模式消除了根源问题。

新的 Detect GUI 版本

Detect GUI 已更新到 2024.1.0 版本，其中包含 Black Duck Detect (CLI) 9.1.0。

支持的浏览器版本

- Safari 版本 17.1.2
  - 不再支持 Safari 版本 14 和更低版本
- Chrome 版本 120.0.6099.216（正式版本）(x86_64)

    - 不再支持 Chrome 版本 91 和更低版本
- Firefox 版本 121.0.1（64 位）
    - 不再支持 Firefox 版本 89 和更低版本
- Microsoft Edge 版本 120.0.2210.121（正式版本）（64 位）
    - 不再支持 Microsoft Edge 版本 91 和更低版本

容器版本

- 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 增强

Black Duck 2024.1.0 中没有新增或更改的 API 请求。有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

二进制扫描程序信息

二进制扫描程序已更新为版本 2023.12.1。

已修复的问题

在此发布中修复了客户报告的以下问题：

- (HUB-37413)。解决了在 AzureFile 中使用上传源代码作为 SC 的问题。彻底移除上传缓存服务，由存储服务取代。

- (HUB-38991)。修复了“扫描”页面在计算代码位置大小时显示不一致的问题。
- (HUB-39012)。修复了一个 REST API 问题，当使用无效值更新组件版本审批状态时，审批状态会被设置为“未审核”。
- (HUB-39160)。修复了以下问题：如果 URL 被篡改，Black Duck 无法验证项目版本是否为项目的一部分。现在这种做法会返回 HTTP 404 错误页面。
- (HUB-39361)。修复了一个问题，即扫描表中时间戳仅显示为工具提示。
- (HUB-39378)。修复了一个问题，即如果组件有多个不同用途的匹配项，对 BOM 组件用途的编辑偶尔会遭到忽略。
- (HUB-39736)。修复了 KB API /component/<uuid>/versions 端点的性能问题。
- (HUB-39864)。修复了一个问题，即如果每个匹配的组件有多个来源，则 BOM 组件编辑可能会删除多个来源，
- (HUB-39948)。修复了 bomengine 死锁问题，原因是同时删除项目和相应的代码位置。
- (HUB-39959)。修复了 IDP URL 或 XML 验证问题。UI 现在可以显示正确的错误信息，如果 IDP 验证失败，也不会更改系统。
- (HUB-39983)。修复了以下问题：重新扫描存储库时，扫描失败可能会在 Black Duck UI 中导致 412 错误。改进了扫描工作流，以便更好地处理扫描过程中出现的错误。
- (HUB-39987)。修复了一个问题，即 SCM 项目版本中的最近扫描日期与更新日期为空。
- (HUB-40104)。修复了一个问题，即如果在用户的产品注册密钥上注册了加密，然后又取消了注册，组件的“加密”选项卡可能会显示空白页。
- (HUB-40667)。修复了一个问题，即“摘要”仪表板视图中按层级显示的项目策略违反无法填充任何信息。
- (HUB-40685)。修复了以下问题：Black Duck 文档缺少检测速率限制参数。
- (HUB-40898)。修复了一个本地化问题，即最大代码段文件大小显示错误的值。

Black Duck SCA 2023.10.x

Black Duck 版本 2023.10.2

公告

目前尚未发布有关 Black Duck 2023.10.2 的新公告。

新增和更改的功能

Black Duck 2023.10.2 中没有新增或更改的功能。

容器版本

- 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 增强

Black Duck 2023.10.2 中没有新增或更改的 API 请求。有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

二进制扫描程序信息

对于 2023.10.2 中的二进制扫描程序没有更改。

已修复的问题

此版本修复了以下问题：

- (HUB-40763)。修复了一个间歇性问题，即如果用户没有立即登录，通过 SSO 页面登录 Black Duck 可能会在一段时间后导致身份验证错误。
- (HUB-40944)。在报告数据库的组件表中，重新添加了缺少的 created_at 与 updated_at 列。
- (HUB-40960)。修复了一个二进制扫描程序捕获清单文件中的构建软件包的问题。

Black Duck 版本 2023.10.1

- 公告
- 新增和更改的功能

公告

文档本地化

2023.7.0 版本的联机帮助和发行说明已本地化为日语和简体中文。

新增和更改的功能

Sigma 版本 2023.9.0 更新

Sigma 2023.9.0 包含扫描 Dockerfile 扩展程序的修复。

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

更新了对匹配的文件 API 请求的响应

以下 API 请求现在会在其响应中包含 uri 字段：

- /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

二进制扫描程序信息

对于 2023.10.1 中的二进制扫描程序没有更改。

已修复的问题

在此发布中修复了客户报告的以下问题：

- (HUB-37681)。已将缺少的公共 API：api/projects/{projectId}/versions/{versionId}/bom-status/{scanId} 添加到《REST API 开发人员指南》。
- (HUB-39616)。更新了 matched-files 查询的 API 响应，以包含 uri 字段。有关更多信息，请参阅 API 增强功能部分。
- (HUB-39693)。使用扫描 cli 时，将与符号链接相关的日志消息移至“跟踪”级别。
- (HUB-40316)。修复了一个问题，即当文件名为空白时，扫描客户端可能无法向 BDIO 文件写入数据。已添加验证功能，以验证存在的是文件名而不是空字符串。
- (HUB-40354)。阐明了有关子项目名称和许可证处理的通知文件报告文档。
- (HUB-40524)。阐明了有关内部托管选项的检测托管位置的文档。
- (HUB-40631)。修复了一个问题，即如果一个项目版本作为子项目添加到另一个项目，而该子项目没有昵称，则在生成版本详细信息报告时可能会出现空指针异常。

Black Duck 版本 2023.10.0

公告

关于 curl 和 libcurl 的安全公告（CVE-2023-38545，CVE-2023-3 8546）

Black Duck 已注意到与 curl 和 libcurl 有关的安全问题，项目维护者和原始创建者于 2023 年 10 月 3 日披露了该问题。

CVE-2023-38545 影响到 7.69.0 至 8.3.0 版本的 curl，并解决了影响 libcurl 和 curl 命令行工具的缓冲区溢出漏洞。溢出可能发生在 SOCKS5 握手期间。如果握手速度较慢，则可能无法解析用户提供的异常长的主机名，而是将其复制到目标缓冲区中，该缓冲区可能会超过分配的大小。此类基于堆的缓冲区溢出已知会导致崩溃、数据损坏甚至任意代码执行。

CVE-2023-38546 与 Cookie 注入漏洞有关，但 curl 维护者表示，由于必须满足一系列条件，漏洞被利用的可能性很低。受此漏洞影响的版本为 7.9.1 至 8.3.0（含）。升级到 curl 8.4.0 可以解决这个问题。建议用

户在每次调用 curl_easy_duphandle(); 之后都调用 curl_easy_setopt(cloned_curl, CURLOPT_COOKIELIST, "ALL");。

我们认为，Black Duck 产品、服务和系统面临的风险有限。在我们已经接触到的风险范畴内，我们已经升级到最新版本的 curl 来修复这种情况。

有关更多信息，请访问：

- 应对严重的 libcurl 和 curl 漏洞 (CVE-2023-38545)
- 如何应对 curl 和 libcurl 漏洞

PostgreSQL 14 容器迁移

Black Duck 2023.10.0 支持从使用 PostgreSQL 11 容器（版本 2022.2.0 至 2022.7.x）或 PostgreSQL 13 容器（版本 2022.10.0 至 2023.7.x）的版本进行升级。在安装过程中，blackduck-postgres-upgrader 容器将现有数据库迁移到 PostgreSQL 14，然后在完成后退出。

强烈建议使用非核心 PG 扩展的客户在迁移前卸载这些扩展，并在迁移成功完成后重新安装；否则，迁移可能会失败。

进行复制设置的客户在迁移之前需要遵循 pg_upgrade 文档中的说明。如果没有进行上述的准备工作，迁移可能会成功，但复制设置将会中断。

不使用 Black Duck 提供的 PostgreSQL 映像的客户不会受到影响。

注意：从 2023.10.0 开始，Black Duck 将仅支持从使用 PostgreSQL 11 或 PostgreSQL 13 容器的 Black Duck 版本（即包含 2022.2.0 和 2023.7.x 二者在内以及介于二者之间的所有 Black Duck 版本）直接升级。对于 Black Duck 提供的 PG 容器的用户，要从较旧的 Black Duck 版本（即 2022.2.0 之前的所有 Black Duck 版本）升级需要执行两步升级：先升级到 2023.7.x，然后再升级到 2023.10.x。

重要提示：开始迁移之前：

- 确保您有额外的 10% 磁盘空间，以避免由于系统目录的数据复制而导致磁盘使用情况出现意外问题。
- 检查根目录空间和卷安装以避免磁盘空间不足，因为这可能导致 Linux 系统中断。

对于 Kubernetes 和 OpenShift 用户：

- 在普通 Kubernetes 上，PostgreSQL Pod 中的 postgres-upgrader init 容器将以 root 身份运行。但是，唯一的要求是容器与 PostgreSQL 数据卷的所有者以相同的 UID 运行。
- 在 OpenShift 上，postgres-upgrader init 容器假定它将使用与 PostgreSQL 数据卷所有者相同的 UID 运行。

对于 Swarm 用户：

- 迁移完全是自动进行的；除了标准的 Black Duck 升级之外，不需要额外的操作。
- blackduck-postgres-upgrader 容器必须以 root 身份运行。
- 随后 Black Duck 重新启动时，blackduck-postgres-upgrader 将确定不需要迁移，并立即退出。

终止对 PostgreSQL 13 的支持

Black Duck 2023.10.0 已终止对 PostgreSQL 13 的支持。有关更多信息，请参阅 PostgreSQL 升级计划页面。

Black Duckctl 的生命周期结束

从 2023.7.0 版本开始，Black Duckctl 不再受支持，也不会再有更新。Black Duckctl 的文档可在 https://github.com/blackducksoftware/hub/tree/master/kubernetes/blackduck 找到。

请注意，Black Duck 2023.7.0 发行说明中意外遗漏了此公告。

针对 PostgreSQL 容器用户的升级限制

Black Duck 2023.10.0 现在仅支持从使用 PostgreSQL 11 或 PostgreSQL 13 容器的 Black Duck 版本（即包含 2022.2.0 和 2023.7.x 二者在内以及介于二者之间的所有 Black Duck 版本）直接升级。对于 Black Duck 提供的 PG 容器的用户，要从较旧的 Black Duck 版本（即 2022.2.0 之前的所有 Black Duck 版本）升级需要执行两步升级：先升级到 2023.7.x，然后再升级到 2023.10.x。

文档本地化

2023.7.0 版本的 UI 已本地化为日语和简体中文。在即将发布的版本中，将提供联机帮助和发行说明的本地化格式。

新增和更改的功能

新增了 GitHub SCM 存储库扫描和只读 BOM

您现在可以将 Black Duck 与 GitHub 存储库集成，以快速轻松地获得 GitHub 中所有存储库的可见性，以及在 Black Duck 中添加项目版本 BOM 的能力。

您现在可以执行以下操作：

- 在 Black Duck 中将选定的主存储库添加为新项目：这使得用户可以快速查看 GitHub 存储库的安全和策略违反情况。
- 随意运行扫描：您可以从映射到存储库的 Black Duck 版本页面触发扫描，以查找当前库中的任何新问题，例如快速查找关键的零日漏洞。此扫描结果会创建一个更轻的只读 BOM，它将提供存储库的快速概览，详细说明找到的组件和许可证，以及与这些组件相关的任何漏洞。

请注意，此功能目前仅支持托管 Black Duck 客户。SCM 集成使用严格在 Kubernetes 环境中运行的服务，无论是原生还是 Kubernetes in Docker (KinD)。需要使用 helm 图表来安装 Black Duck 才能使用此功能。

新增了扫描自动取消映射管理页面

现在，您可以管理计划何时从非活动项目版本取消映射扫描。它们需要满足项目版本阶段和不活动时间条件，并且只有在宽限期过后才会取消映射。单击“管理”按钮→“系统设置”→“数据保留”→“扫描自动取消映射”，可在 Black Duck 中找到“扫描自动取消映射”页面。

新增了自动扫描重试标头支持 Black Duck Detect

429 响应中增加了新的 Retry-After 标头，以便 Detect 知道何时再次尝试速率限制扫描。以下属性已添加到 blackduck-config.env 文件：

BLACKDUCK_USE_QUEUE_RATE_LIMITING：设为 true，在环境中启用队列基本速率限制。默认值为 false。

BLACKDUCK_INITIAL_RATE_LIMIT_DURATION_BRACKET_THRESHOLD_MINUTES：指示系统从第一次重试持续时间移动到第二次重试持续时间之前，系统必须进行速率限制的持续时间。

BLACKDUCK_RATE_LIMIT_DURATION_THRESHOLD_BRACKET_INCREMENT_MINUTES：指示系统在进入下一个重试持续时间和乘数之前，在速率限制区间内的停留时间。

BLACKDUCK_INITIAL_RETRY_DURATION_MINUTES：第一个速率限制区间内的 Retry-After 标头的初始持续时间。

BLACKDUCK_RETRY_DURATION_MULTIPLIER_MINUTES：每次系统达到新的速率限制持续时间时，重试后持续时间乘以的数值。

新增了运行时阈值环境变量

您现在可以通过将以下变量添加到 blackduck-config.env 文件来配置阈值以确定长时间运行作业：

- BLACKDUCK_DEFAULT_JOB_RUNTIME_THRESHOLD_HOURS={value in hours}

此环境变量的默认值为 24 小时。

新增了报告中包含子项目选项

现在，在创建以下报告时，您可以在报告生成对话框中选中新的包含子项目复选框，选择包含子项目：

- 通知文件
- SBOM
- 版本详细信息

请注意，此功能默认处于启用状态，在此更改之前，子项目已包含在报告生成中。此功能现在显式允许您配置此功能。

新增了过渡升级指南

请注意，此功能是在 Black Duck 2023.1.0 中添加的，但在该版本的发行说明中意外遗漏了此功能。

解决安全风险的最简单方法是升级漏洞较少的所用组件版本。对于用作直接匹配的组件，这样更容易。如果不了解组件中引入的根直接依赖项，这将更加难以减轻或消除作为过渡依赖项引入的组件漏洞。此功能的目标是更简单、直接地提供过渡升级指南，以提供更好的开发人员体验和更明确的行动呼吁。

增强了 Black Duck Secure Container (BDSC)

Black Duck 引入了一种新型容器映像扫描和项目视图，以简化容器映像的风险管理。容器项目可以显示汇总的 BOM 和风险，但也提供了一种逐层查看风险的方法，包括将风险从基础映像或操作系统和应用层中分离出来。此外，我们还增加了对查看组件在层中添加或删除的位置和时间的支持。

此外，Black Duck KnowledgeBase 还将扩展其清单，以涵盖 Docker Hub 基本容器映像和逐层组件详细信息，从而使 Black Duck 能够将扫描重点放在客户端容器上。

作为特征扫描、二进制扫描和 Docker Inspector 的一部分，现有的 Black Duck 容器映像扫描没有变化，将继续受到支持。新的容器映像扫描功能和项目视图将改善管理容器中发现的风险的用户体验，使客户能够按容器层管理风险。

请注意，要利用此功能，您必须在产品注册密钥上启用 Black Duck Secure Container (BDSC)。对于订阅 Black Duck Binary Analysis 集成功能的客户，其许可证中将包含此功能。

增强了许可证风险聚合 - 有限的客户可用性

在此增强之前，无法在父项目中跟踪或查看子项目的许可证风险。这就造成了在使用子项目层次结构时可能会遗漏许可证风险。现在，启用此功能后，项目 BOM 中显示的子项目的许可证风险将由子项目的许可证风险及其组件的最高许可证风险决定。

请注意，此功能并非普遍可用，默认情况下也不启用。增强的许可证风险聚合将在即将发布的 Black Duck 版本中普遍可用，届时将默认启用。

增强了 SBOM 导入组件可见性

现在，您可以识别哪些组件源自 SBOM 导入，哪些源自其他类型的识别/扫描或其他导入的 SBOM。在项目版本的“来源”选项卡中，您可以识别 SBOM 类型（SPDX 或 CycloneDX）、导入 SBOM 的时间、SBOM 的提供者以及用于创建 SBOM 的工具版本。

增强了组件版本页面

现在，“组件版本”页面可根据系统管理员设置的评分系统优先级，更清楚地显示您在查看的安全风险。现在，表会显示某个组件版本是否存在其他漏洞，以及有多少漏洞来自其他评分系统，如 CVSS v2。

增强了作业页面功能

作业页面的“处理”选项卡现在会在运行时间超过正常时间的作业旁边显示一个警告图标。您还可以根据长时间运行的作业过滤此页面，以显示这些作业的列表。

此外，用户还可以使用新的 Prometheus 指标来查看系统中运行时间超过平常的作业。

扫描硬件要求变化

Black Duck 2023.10.0 扫描硬件要求将发生一些变化，因此 Black Duck 客户必须更新其环境，并在必要时根据以下指南分配额外的硬件资源。请参阅 Black Duck 硬件扩展指南，以便在这些建议发生更改时及时了解最新情况。

表 2: 硬件扩展指南

名称	详细信息	
10sph	扫描次数/小时：50 SPH 百分比增加：400% API/小时：2,500 项目版本：10,000	IOPS：读取：15,000/写入：9,000 Black Duck 服务：CPU：10 核/内存：36GB PostgreSQL：CPU：2 核/内存：8 GB 总数：CPU：12 核/内存：44GB
120sph	扫描次数/小时：120 SPH 百分比增加：0% API/小时：3,000 项目版本：13,000	IOPS：读取：15,000/写入：15,000 Black Duck 服务：CPU：11 核/内存：56GB PostgreSQL：CPU：4 核/内存：16 GB 总数：CPU：15 核/内存：72 GB
250sph	扫描次数/小时：300 SPH 百分比增加：20% API/小时：7,500 项目版本：15,000	IOPS：读取：15,000/写入：15,000 Black Duck 服务：CPU：16 核/内存：85GB PostgreSQL：CPU：6 核/内存：24 GB 总数：CPU：22 核/内存：109GB
500sph	扫描次数/小时：650 SPH 百分比增加：30% API/小时：18,000 项目版本：18,000	IOPS：读取：25,000/写入：25,000 Black Duck 服务：CPU：23 核/内存：133GB PostgreSQL：CPU：16 核/内存：64GB 总数：CPU：39 核/内存：197GB
1000sph	扫描次数/小时：1400 SPH 百分比增加：40% API/小时：26,000 项目版本：25,000	IOPS：读取：25,000/写入：25,000 Black Duck 服务：CPU：44 核/内存：367GB PostgreSQL：CPU：22 核/内存：88GB 总数：CPU：66 核/内存：455GB
1500sph	扫描次数/小时：1600 SPH 百分比增加：6% API/小时：41,000 项目版本：28,000	IOPS：读取：25,000/写入：25,000 Black Duck 服务：CPU：53 核/内存：464GB PostgreSQL：CPU：26 核/内存：104 GB 总数：CPU：79 核/内存：568GB
2000sph	扫描次数/小时：2300 SPH 百分比增加：15% API/小时：50,000 项目版本：35,000	IOPS：读取：30,000/写入：30,000 Black Duck 服务：CPU：64 核/内存：565GB PostgreSQL：CPU：32 核/内存：128GB 总数：CPU：96 核/内存：693GB

表 3: PostgreSQL 设置

名称	详细信息	
10sph	扫描次数/小时：50 PostgreSQL CPU/内存：2 核/内存：8 GB	autovacuum_max_workers：4 maintenance_work_mem (MB)：512

名称	详细信息	
	shared_buffers (MB)：2654 effective_cache_size (MB)：3185	max_connections：400 work_mem (MB)：50
120sph	扫描次数/小时：120 PostgreSQL CPU/内存：CPU：4 核/内存：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	扫描次数/小时：300 PostgreSQL CPU/内存：CPU：6 核/内存：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	扫描次数/小时：650 PostgreSQL CPU/内存：CPU：16 核/内存：64GB 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	扫描次数/小时：1400 PostgreSQL CPU/内存：CPU：22 核/内存：88GB 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	扫描次数/小时：1600 PostgreSQL CPU/内存：26 核/内存：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	扫描次数/小时：2300 PostgreSQL CPU/内存：32 核/内存：128GB 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

更新了存档项目版本阶段的策略评估

对存档项目版本阶段进行了以下更改：

- 项目版本阶段的策略表达式不再允许将“存档”作为值。
- 包含项目版本阶段和“存档”值的现有策略规则将被自动禁用。
- 新的策略规则和表达式更改将不再在“存档”阶段的项目版本中计算。

更新了 PostgreSQL 设置

从 Black Duck 2023.10.0 开始，PostgreSQL 设置将在使用 PostgreSQL 容器的部署中自动设置。使用外部 PostgreSQL 的客户仍需手动应用设置。

更新了 Black Duck 托管的 Detect 版本

Black Duck 2023.10.0 现在在 Black Duck Detect 页面上提供对 Black Duck Detect 9 的支持，对 Detect 7.x 的支持已经结束。升级到 Black Duck 2023.10.0 后，当前使用 Detect 7.x 的客户将看到一个警告指示灯，指示 Detect 7.x 已达到支持极限，建议升级。请注意，更改此配置后将无法恢复到 Detect 7.x。

更新了 Artifactory 和 SCM 集成要求

要在环境中使用 Artifactory 和 SCM 集成，必须在注册密钥中启用这些功能。启用后，必须在 values.yaml 文件中添加以下内容：

```
enableIntegration: true
```

更新了 SCA 即服务部署文件

用于 SCA 即服务的部署文件已更新如下：

- 将 RabbitMQ 映像从 1.2.14 更新至 1.2.29
- 添加了新的环境变量，以配置端口进行正确通信：
  - BLACKDUCK_RABBIT_LISTENERS_PORT: "5672"
  - BLACKDUCK_RABBIT_MANAGEMENT_PORT: "15672"

更新了显示不匹配组件的功能

用于确定是否在项目版本组件视图中显示“不匹配组件”计数的 BLACKDUCK_HUB_SHOW_UNMATCHED 属性现在默认启用。

请注意，此更改是在 Black Duck 2023.7.0 中进行的，但在该版本的发行说明中意外遗漏。

更新了 SBOM 字段的审计跟踪

项目的“活动”选项卡现在将报告对以下 SBOM 字段的添加或修改情况：

- 软件包供应商名称
- 软件包供应商电子邮件
- 软件包供应商类型

更新了报告数据库表

下表已更新：

- created_at 列已添加到 component_policies 表。此列包含创建策略违反时的次数列表。
- purl 列已添加到 component 表。此列包含组件的软件包 URL。

更新了报告数据库

通过 API 获取的存储为 channel_release_external_namespace 的详细信息现在也可以通过报告数据库的组件表获取。它声明了来源的通用名称空间（maven、debian、ubuntu 等）。

更新了登录页面和框架

围绕 Black Duck 的登录页面和框架已更新。

更新了容器扫描功能名称

Black Duck Container Scanning — Limited Customer Availability 已更名为 Black Duck Secure Container (BDSC)。 Black Duck Secure Container 扫描提供了识别容器映像中的组件、其层和基础映像的功能。

产品注册页面已相应更新。

增加了 Kubernetes 上的默认存储服务大小

Black Duck 2023.10.0 将容器大小和 Java 堆大小从 1 GB 存储空间/512 MB 内存增加到 2 GB 存储空间/1 GB 内存。

容器版本

- 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 增强

增强了 REST API 请求的页面导航功能

返回分页结果的 REST API 现在以相同的顺序提供指向其他页面的链接，以帮助遍历数据。

更新了 GET/api/jobs-runtimes 请求

现在，我们在 GET /api/jobs-runtimes 响应中包含了作业是否长时间运行的信息。

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

longRunningThresholdMs 值决定了作业类型的运行时阈值。如果作业超过此限制，则视为长时间运行。longRunning 值根据作业的运行时间和先前作业运行的持续时间确定作业是否长时间运行。

提高了 /api/project 请求的性能

以下 API 请求的性能得到了提高：

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

二进制扫描程序信息

二进制扫描程序已更新为版本 2023.9.3。

- 现在支持容器扫描。

已修复的问题

在此发布中修复了客户报告的以下问题：

- (HUB-27209)。修复了由于没有 CVSS 2.0 评分的漏洞导致 KB 更新作业失败的问题。
- (HUB-32753)。修复了上传缓存清理无法处理过时的 docker 检查器上传的问题。
- (HUB-33560)。存档项目阶段的策略规则被禁用。任何违反规则的组件都将被清除（即使在存档的项目版本中）。新政策规则不会在“存档”的项目版本中计算。表达式更改不会在“存档”的项目版本中计算。禁用和删除的策略规则 - 已在“存档”的项目版本中清除。
- (HUB-35760)。修复了“扫描”页面上的 Complete 过滤器错误地显示当前正在进行的扫描的问题。
- (HUB-35836)。修复了以下问题：对项目没有任何其他直接访问权限的用户可以删除项目所有者用户，从而将没有直接访问权限的用户分配为项目的项目经理角色。现在，无法直接访问项目的用户将被阻止从该项目中删除用户。
- （HUB-38385，HUB-38654）。修复了与传统扫描处理方法有关的超时问题。
- (HUB-38595)。更新了 REST API 开发人员指南中 GET /api/codelocations/{codeLocationId}/latest-scan-summary 请求的示例响应。
- (HUB-38682)。修复了以下问题：单击“来源”列下的 BOM 视图中的“N 个匹配”链接时，不会清除“来源”选项卡中的先前选择，并显示先前记住的匹配文件夹/文件。
- (HUB-38753)。修复了批量编辑组件版本用法可能会错误地无法更新策略违反的问题。
- (HUB-38766)。修复了项目查看器用户可以访问项目的设置页面并对项目进行更新的问题。通过此修复，没有权限的项目查看器用户仍可访问项目设置页面，但现在将无法更新任何内容。所有更新/删除操作都将被禁用。
- (HUB-38803)。修复了在 BOM 页面上单击未确认的代码段链接时，标记为“已忽略”的代码段仍会显示的问题。单击此链接将自动应用“匹配忽略”：“代码段”页面的“未忽略”筛选器。
- (HUB-38806)。修复了通过 API 修复 BDSA-2023-1225 漏洞可能会生成 HTTP 404 错误的问题。
- (HUB-38841)。修复了“组件许可证”模式的许可证注释和归因声明中的文本大小。
- (HUB-38878)。修复了发生组件合并时可能从 BOM 中删除组件的问题。

- (HUB-39079)。修复了尝试呈现大型 HTML 报告可能会生成 HTTP 503 服务不可用服务器错误响应的问题。现在，尝试呈现大型 HTML 报告将生成包含实际报告大小和当前限制的验证错误。当前限制由 HUB_MAX_HTML_REPORT_SIZE_KB 环境变量决定，默认设置为 3000 KB。
- (HUB-39275)。修复了以下问题：如果在 UI 中将未映射的扫描保留时间设置为 365 天以上，则在运行清除作业时会将其重置为 30 天。
- (HUB-39318)。修复了无法在特定组件版本的“版权”选项卡中突出显示来源的问题。
- (HUB-39368)。修复了当用户单击其他选项卡时，全局搜索会覆盖当前所选搜索的查询的问题。搜索请求现在不会持久存在，这意味着如果用户刷新浏览器，或注销后再重新登录，以前的过滤器将不会被记住。
- (HUB-39441)。修复了 ScmServerAppService 在初始化时仅检查 scm 集成注册密钥的问题。
- (HUB-39496)。修复了以下问题：如果文件大小超过 16 GB，BDBA 扫描生成的 BDIO 可能无法上传到 Black Duck。该限制已增加到 90GB。
- (HUB-39744)。修复了 KBUpdateWorkflowJob 运行后，BOM/版本页面和仪表板上显示的漏洞结果之间的差异问题。
- (HUB-39836)。修复了 component_matches 具体化视图不包含所有匹配类型的问题。
- (HUB-39864)。修复了编辑具有多个来源（在鼠标悬停时可见）的 BOM 组件（更改用法或注释）可能会删除所有来源的问题。
- (HUB-40060)。修复了编辑 BOM 中具有多个来源的组件时的问题，选择仅限于 10 个来源。该数字已增加到 100。
- (HUB-40085)。修复了创建报告时的性能问题，因为生成报告的时间可能比预期的要长得多，从而导致管道中的等待时间过长。

Black Duck SCA 2023.7.x

Black Duck 版本 2023.7.3

公告

关于 curl 和 libcurl 的安全公告（CVE-2023-38545，CVE-2023-3 8546）

Black Duck 已注意到与 curl 和 libcurl 有关的安全问题，项目维护者和原始创建者于 2023 年 10 月 3 日披露了该问题。

CVE-2023-38545 影响到 7.69.0 至 8.3.0 版本的 curl，并解决了影响 libcurl 和 curl 命令行工具的缓冲区溢出漏洞。溢出可能发生在 SOCKS5 握手期间。如果握手速度较慢，则可能无法解析用户提供的异常长的主机名，而是将其复制到目标缓冲区中，该缓冲区可能会超过分配的大小。此类基于堆的缓冲区溢出已知会导致崩溃、数据损坏甚至任意代码执行。

CVE-2023-38546 与 Cookie 注入漏洞有关，但 curl 维护者表示，由于必须满足一系列条件，漏洞被利用的可能性很低。受此漏洞影响的版本为 7.9.1 至 8.3.0（含）。升级到 curl 8.4.0 可以解决这个问题。建议用

户在每次调用 curl_easy_duphandle(); 之后都调用 curl_easy_setopt(cloned_curl, CURLOPT_COOKIELIST, "ALL");。

我们认为，Black Duck 产品、服务和系统面临的风险有限。在我们已经接触到的风险范畴内，我们已经升级到最新版本的 curl 来修复这种情况。

有关更多信息，请访问：

- 应对严重的 libcurl 和 curl 漏洞 (CVE-2023-38545)
- 如何应对 curl 和 libcurl 漏洞

新增和更改的功能

容器版本

注意：nginx v2.0.61 和 upload-cache v1.0.49 映像是专门为 2023.7.3 创建的，用于解决 curl 漏洞，并且只能与 2023.7.3 一起部署。它们与 Black Duck 2023.10.0 不兼容。

- 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 增强

Black Duck 2023.7.3 中没有新增或更改的 API 请求。有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

二进制扫描程序信息

对于 2023.7.3 中的二进制扫描程序没有更改。

已修复的问题

在此发布中修复了客户报告的以下问题：

- (HUB-40080)。修复了以下问题：用于更新 reporting.component_vulnerability 视图的刷新具体化视图查询可以从多个不同的 ReportingDatabaseTransferJobs 并行执行多次。

Black Duck 版本 2023.7.2

公告

目前尚未发布有关 Black Duck 2023.7.2 的新公告。

新增和更改的功能

Black Duck 2023.7.2 中没有新增或更改的功能。

API 增强

Black Duck 2023.7.2 中没有新增或更改的 API 请求。有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

二进制扫描程序信息

对于 2023.7.2 中的二进制扫描程序没有更改。

已修复的问题

在此发布中修复了客户报告的以下问题：

- (HUB-39559)。修复了每次服务器启动时错误触发加密密钥轮换的问题。此外，还修复了 SAML 私钥未包含在加密密钥轮换中的问题。

Black Duck 版本 2023.7.1

公告

即将发生的扫描硬件要求变化

Black Duck 2023.10.0 扫描硬件要求将发生一些变化，因此 Black Duck 客户需要更新其环境，并在必要时根据以下指南分配额外的硬件资源。

表 4: 硬件扩展指南

名称	详细信息	
10sph	扫描次数/小时：50 SPH 百分比增加：400% API/小时：2,500 项目版本：10,000	IOPS：读取：15,000/写入：9,000 Black Duck 服务：CPU：10 核/内存：36GB PostgreSQL：CPU：2 核/内存：8 GB 总数：CPU：12 核/内存：44GB
120sph	扫描次数/小时：120 SPH 百分比增加：0% API/小时：3,000 项目版本：13,000	IOPS：读取：15,000/写入：15,000 Black Duck 服务：CPU：11 核/内存：56GB PostgreSQL：CPU：4 核/内存：16 GB 总数：CPU：15 核/内存：72 GB
250sph	扫描次数/小时：300 SPH 百分比增加：20% API/小时：7,500 项目版本：15,000	IOPS：读取：15,000/写入：15,000 Black Duck 服务：CPU：16 核/内存：85GB PostgreSQL：CPU：6 核/内存：24 GB 总数：CPU：22 核/内存：109GB
500sph	扫描次数/小时：650 SPH 百分比增加：30% API/小时：18,000 项目版本：18,000	IOPS：读取：25,000/写入：25,000 Black Duck 服务：CPU：23 核/内存：133GB PostgreSQL：CPU：16 核/内存：64GB 总数：CPU：39 核/内存：197GB
1000sph	扫描次数/小时：1400 SPH 百分比增加：40% API/小时：26,000 项目版本：25,000	IOPS：读取：25,000/写入：25,000 Black Duck 服务：CPU：44 核/内存：367GB PostgreSQL：CPU：22 核/内存：88GB 总数：CPU：66 核/内存：455GB
1500sph	扫描次数/小时：1600 SPH 百分比增加：6% API/小时：41,000 项目版本：28,000	IOPS：读取：25,000/写入：25,000 Black Duck 服务：CPU：53 核/内存：464GB PostgreSQL：CPU：26 核/内存：104 GB 总数：CPU：79 核/内存：568GB
2000sph	扫描次数/小时：2300 SPH 百分比增加：15% API/小时：50,000 项目版本：35,000	IOPS：读取：30,000/写入：30,000 Black Duck 服务：CPU：64 核/内存：565GB PostgreSQL：CPU：32 核/内存：128GB 总数：CPU：96 核/内存：693GB

表 5: PostgreSQL 设置

名称	详细信息	
10sph	扫描次数/小时：50 PostgreSQL CPU/内存：2 核/内存：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	扫描次数/小时：120 PostgreSQL CPU/内存：CPU：4 核/内存：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	扫描次数/小时：300 PostgreSQL CPU/内存：CPU：6 核/内存：24 GB	autovacuum_max_workers：6 maintenance_work_mem (MB)：1024 max_connections：500

名称	详细信息	
	shared_buffers (MB)：8016 effective_cache_size (MB)：9619	work_mem (MB)：35
500sph	扫描次数/小时：650 PostgreSQL CPU/内存：CPU：16 核/内存：64GB 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	扫描次数/小时：1400 PostgreSQL CPU/内存：CPU：22 核/内存：88GB 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	扫描次数/小时：1600 PostgreSQL CPU/内存：26 核/内存：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	扫描次数/小时：2300 PostgreSQL CPU/内存：32 核/内存：128GB 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

新增和更改的功能

新的 Artifactory 配置管理

现在，您可以在 Black Duck UI 中管理 Artifactory 集成配置。为此，请以集成经理用户身份登录，单击“管理”按钮，然后选择“集成”。

因此，许多环境属性已被移除，现在可以在 Black Duck UI 中进行配置。下列属性已被移除：

- 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

适用于 Artifactory 集成服务的新 Docker 映像/容器

添加了新的 Docker 映像/容器，用于 Artifactory 集成。在部署此映像/容器之前，托管的 Black Duck 客户必须使用其注册密钥启用 Artifactory 集成。

适用于 Artifactory 集成的新 SCA 引擎属性

现在必须将以下 environs 属性添加到 Black Duck 的 values.yaml 文件中，以便 Black Duck 和 sca-engine-as-a-service 能够相互通信：

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

注意：虽然这些属性必须添加到 values.yaml 文件中，但不需要立即设置它们的值，可以保留为空，如上例所示。BLACKDUCK_SCA_ENGINE_HOST 的值会根据您计划命名的 sca-engine-as-a-service 部署而变化。

新用户角色

新用户角色已添加到总体角色列表中：

- 集成经理：此角色授予管理所有集成的能力。
- 轻量级 BOM 代码扫描程序：此角色授予对轻量级 BOM 的管理权限。
- 轻量级 BOM 项目经理：此角色授予对轻量级 BOM 项目的管理权限。
- 轻量级 BOM 项目版本经理：此角色授予对轻量级 BOM 项目版本的管理权限。

更新了全代码段扫描功能

随着代码段扫描使用的增加，我们开始注意代码段扫描的性能和可扩展性问题。为了帮助缓解这些问题，我们正在实现战术限制和优化，以管理吞吐量并减少代片段匹配的冗余重复工作：

- 将允许的最大代码段文件大小范围减少到 1-4MB（原为 1-16MB）
- 将最大代码段文件大小的默认值更改为 1MB（原为 2MB）

此外，现在必须在您的注册密钥上激活全代码段扫描选项。受影响的 Detect 参数包括：

detect.blackduck.signature.scanner.snippet.matching

- FULL_SNIPPET_MATCHING
- FULL_SNIPPET_MATCHING_ONLY

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

通过 pURL API 请求查找新组件元数据

以下 API 请求可用于将软件包 URL 作为搜索条件搜索单个组件。响应提供端点来获取有关组件、版本和变体的详细信息：

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

更新了组件 API 端点响应

以下组件 API 端点的响应已更新，包含请求中使用的 bomMatchInclusion 过滤选项（true 或 false）：

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

二进制扫描程序信息

对于 2023.7.1 中的二进制扫描程序没有更改。

已修复的问题

在此发布中修复了客户报告的以下问题：

- (HUB-38374)。修复了 Black Duck SCM 集成在使用不同的日期/时间格式时，可能导致在尝试拉取存储库时出错的问题。
- (HUB-38790)。修复了某些迁移脚本导致语法错误的问题。

- (HUB-38968)。修复了以下问题：由于名称空间 UUID 值不遵循 SBOM 最佳实践，而将 SBOM 上传到 Black Duck 可能失败。
- (HUB-39026)。修复了在运行 Detect 8 或使用 BDIO 聚合时，默认启用的不匹配组件标记错误地计算软件包文件数的问题。这导致由于 BDIO 文件中的层次结构，运行的软件包管理器数量被添加到未匹配组件计数中。
- (HUB-39072)。修复了 REST API 文档中的 BOM 组件漏洞修复表示的 CreatedAt 和 UpdatedAt 定义，声明它们是将漏洞添加到 BOM 组件源位置或在 BOM 组件源上更新的日期。
- (HUB-39168)。修复了一个 UI 问题：“添加过滤器”和“过滤器版本…”文本字段选项可能会因修改的组件而消失，并且在修改组件时漏洞历史记录图可能会消失。
- (HUB-39211)。修正了日语本地化中策略覆盖日期信息显示不正确的问题。
- (HUB-39274)。修复了以下问题：KbUpdateJob 未验证客户产品注册中的 BDSA 许可，这可能会导致在请求期间出现 HTTP 403 禁止响应。
- (HUB-39367)。修复了许可证名称包含 "" 可能导致 KbUpdateWorkflowJob-License 更新失败的问题。

Black Duck 版本 2023.7.0

公告

终止对 Docker 18.09.x 和 19.03.x 的支持。

对 Docker 18.09.x 和 19.03.x 的支持已在 Black Duck 2023.7.0 版本后结束。Docker 20.10.x 将是唯一支持的版本。

即将移除 gen02 大小调整指南

Black Duck 2023.10.0 将移除 gen02 调整指南和文档。有关调整参考资料，请参阅 Black Duck 硬件扩展指南页面。

即将终止对 PostgreSQL 13 的支持

随着 2023.10.0 版本即将发布，Black Duck 将结束对外部 PostgreSQL 13 的支持。请参阅 Black Duck 2023.10.0 版本。有关更多信息，请参阅 PostgreSQL 升级计划页面。

PostgreSQL 容器即将迁移到版本 14

Black Duck 将在 2023.10.0 版本中将其 PostgreSQL 映像迁移到版本 14。不使用 Black Duck 提供的 PostgreSQL 映像的客户不会受到影响。

即将针对 PostgreSQL 容器用户的升级限制

从 2023.10.0 开始，Black Duck 将仅支持从使用 PostgreSQL 11 或 PostgreSQL 13 容器的 Black Duck 版本（即包含 2022.2.0 和 2023.7.x 二者在内以及介于二者之间的所有 Black Duck 版本）直接升级。对于 Black Duck 提供的 PG 容器的用户，要从较旧的 Black Duck 版本（即 2022.2.0 之前的所有 Black Duck 版本）升级需要执行两步升级：先升级到 2023.7.x，然后再升级到 2023.10.x。

文档本地化

2023.4.0 版本的 UI、联机帮助和发行说明已本地化为日语和简体中文。

新增和更改的功能

对外部数据库的 PostgreSQL 15 支持

Black Duck 对于使用外部 PostgreSQL 的新安装，现在支持并建议使用 PostgreSQL 15。PostgreSQL 15 在 Azure Database for PostgreSQL 上尚不受支持，因此 Black Duck 建议该环境的用户使用 PostgreSQL 14 Flexible Server。

迁移到 Black Duck2023.7.x 不需要迁移到 PostgreSQL 15。

内部 PostgreSQL 容器的用户无需执行任何操作。

报告对象类型的加密

Black Duck 2023.7.0 现在将存储在对象存储中的报告对象标记为敏感对象，使这些对象有资格在保留它们的 FILE 卷中进行静态加密。为了对这些对象进行加密，必须在您的环境中启用 Black Duck Crypto，并提供适当的密钥。将根据您的环境的 Black Duck Crypto 设置应用以下行为更改：

对于在升级到 2023.7.0 时未启用 Black Duck Crypto 的环境

所有现有报告和所有新报告都将在磁盘上保持未加密状态 - 但标记为敏感对象。如果以后启用 Black Duck Crypto，这些对象将在后台加密，以符合其敏感性质。

对于在升级到 2023.7.0 时已启用 Black Duck Crypto 的环境

如果您已启用 Black Duck Crypto，则现有报告将保持未加密状态，而所有新报告都将加密。如果您需要强制加密所有内容，请设置环境变量 SYNOPSYS_CRYPTO_ROTATE_RESOURCES_ON_STARTUP=true 这将强制系统轮换内部密钥并重新加密所有内容，包括旧的未加密报告。

存储服务对象的加密

如果启用了 Black Duck Crypto，将对存储在对象存储 FILE 卷中的敏感对象进行静态加密。

更新了“作业”页面

重新设计了“作业”页面，以提高所显示信息的可用性和可扩展性。“作业”页面已分解为三个选项卡：

- 已完成：显示所有已完成、已成功或已失败的作业。
- 已安排：显示已安排在您的环境中运行的所有作业。
- 正在处理：显示当前正在处理的所有作业。

新的“不匹配的来源”管理页面

现在，您可以更轻松地管理 Black Duck 在软件包扫描过程中识别但无法映射到组件版本的来源 ID。在“不匹配的来源”页面中，您可以添加或移除与自定义组件的映射，这些映射随后将添加到后续的软件包管理器扫描中。可以通过单击“管理”>“不匹配的来源”访问“不匹配的来源”页面。

此外，您现在还可以在自定义组件的组件版本页面上管理映射到这些组件的来源 ID。

与自定义组件匹配需要使用 Detect 7 或更高版本，目前仅支持软件包管理器扫描。

增强了“通知文件”报告

可添加到“通知文件”报告中的新选项包括：

- 深度许可证数据：通过组件来源发现的深度许可证。仅在为项目启用了深度许可证时才可用。
- 文件版权文本：在文件匹配中发现的版权文本。仅当存在文件匹配时才可用。
- 不匹配的文件发现：与项目中的组件无关的文件发现。仅当项目中存在不匹配的文件时才可用。
- 文件许可证数据：在文件匹配中发现的许可证。仅当存在文件匹配时才可用。

新的 SBOM 报告字段

SBOM 报告的 SPDX 版本现在包括两个新的可选字段：

- 软件包注释：关于所描述的软件包的一般注释。
- 软件包有效期截止日期：供应商提供的软件包的支持期的结尾。

您必须先在“管理”>“SBOM”>“BOM 组件”下激活这些字段。在启用后，您可以通过导航到项目版本的 BOM，单击组件行末尾的选项按钮，然后选择“SBOM 字段”来更新它们。

更新了 BOM 过滤器标签

BOM 项目版本页面“组件”选项卡上的“匹配状态”过滤器命名不明确。此过滤器仅适用于代码段匹配，因此名称已更改为“代码段匹配状态”，以正确捕获该非常特定的使用案例。

增强了日志记录信息

添加了用户使用用户名/密码登录时用于记录成功和失败登录的日志记录信息（身份验证容器）。

更新了对报告（包含已删除项目）的访问权限

更新了对报告的访问权限，如果其中一个项目已被删除，并且如果用户对报告中的所有剩余项目（尚未删除）拥有权限，或者全局项目读取访问权限是其用户角色的组成部分，则此类用户可以访问该报告。不属于上述任一类别的用户将无法访问该报告。

增强了“版本详细信息”报告

“版本详细信息”报告现在包括对子项目的更新：

- “版本详细信息”更新指南报告现在包括对子项目的升级指南。
- 项目版本更新指南报告的第一列现在为“使用者”，如果不是空白，则报告升级指南的子项目。

增强了报告生成功能

改进了报告数据收集和报告格式编写的机制，以限制内存占用。请注意，由于此更改，可能会导致报告生成时间更长。

KnowledgeBase 环境变量的整合

Black Duck 具有各种环境变量，用于控制各种 KnowledgeBase 服务的 KnowledgeBase 方案、主机和端口配置。从 Black Duck 2023.7.0 开始，KnowledgeBase 环境变量配置已统一在以下变量上，以简化配置：

- BLACKDUCK_KB_SCHEME
- BLACKDUCK_KB_HOST
- BLACKDUCK_KB_PORT

以下属性前缀已被明确移除，并且不再引用：

- BLACKDUCK_KBCLOUD

- BLACKDUCK_KBDETAIL
- BLACKDUCK_JSONWEBTOKEN

已手动覆盖旧 KnowledgeBase 环境变量以进行自定义的用户，应该验证其环境，以确保功能正常。

更新了 UI 中的日期选取器工具

UI 中使用的日期选取器已更新，这将更改其外观（取决于浏览器）和功能。请注意，该工具不会通过浏览器语言进行本地化（Firefox 除外）。现在，该工具的本地化取决于 Chrome、Edge 和 Safari 的操作系统区域设置。

支持的浏览器版本

- Safari 版本 16.4
  - 不再支持 Safari 版本 14 和更低版本
- Chrome 版本 114.0.5735.198（正式版本）(x86_64)
  - 不再支持 Chrome 版本 91 和更低版本
- Firefox 版本 114.0.2（64 位）
  - 不再支持 Firefox 版本 89 和更低版本
- Microsoft Edge 版本 114.0.1823.67（正式版本）（64 位）
  - 不再支持 Microsoft Edge 版本 91 和更低版本

容器版本

- 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 增强

移除 PUT /api/settings/data-retention

如 2023.4.0 发行说明中所述，PUT /api/settings/data-retention 已被弃用，改为使用 PATCH /api/settings/data-retention，如果调用前者，将返回 HTTP 405 METHOD_NOT_ALLOWED 错误消息。现在已在 Black Duck 2023.7.0 中将该 API 完全移除，如果使用它，将返回 HTTP 404 NOT_FOUND 错误消息。

弃用 GET api/external-config/detect-uri

GET api/external-config/detect-uri API 请求已被弃用，改为使用 GET api/settings/detect。虽然该旧版 API 已被弃用，但用户仍然可以使用它。

虽然 GET api/external-config/detect-uri 已被弃用，但没有角色、经过身份验证的用户仍然可以使用它来获取 API 字符串。如果这些用户使用 GET api/settings/detect API，他们将获得 detectUri（如果已设置），不会获得任何其他内容。

改善了 PUT /api/policy-rules/{policyRuleId} 的性能

通过将策略配置文件计算限制为仅在评估项目版本中的组件后发现违规更改时运行，改善了 PUT /api/policy-rules/{policyRuleId} API 请求的性能。

更新了 POST api/components/{componentId}/versions

已更新 POST api/components/{componentId}/versions API 请求，允许用户在创建时将外部 ID 映射到新的自定义组件版本。

新的公共 SBOM 字段端点

PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/sbom-fields 端点现可更新 BOM 组件的 sbom 字段已保存的值。

二进制扫描程序信息

二进制扫描程序已更新为版本 2023.6.0。

- 现在支持扫描 package-lock.json 文件，与以前的扫描相比，该文件可以显示其他组件标识。因此，识别的组件可能会增加。

已修复的问题

在此发布中修复了客户报告的以下问题：

- (HUB-21449)。修复了以下问题：在缓解违规时，嵌套组件中漏洞计数的策略违反显示不正确。
- (HUB-33362)。修复了以下问题：在尝试使用 XML 文件设置 SAML 时，除非禁用 SAML，否则不会保存该文件。
- (HUB-34720)。修复了以下问题：在修改许可证时，例如，在不更改许可证 ID 的情况下，为了反映原始许可证文本而不是通用许可证文本，未将该更改导出到 SPDX 文件。
- (HUB-35512)。修复了以下问题：在 BOM 页面中手动添加具有相同组件+版本+来源的组件版本时，即便移除了来源设置，也会始终显示“无法添加手动 BOM 组件，因为它已经存在。” 错误消息。
- (HUB-37067)。从“查找”→“漏洞”页面中移除了“修复状态”过滤器。
- (HUB-37626)。修复了以下问题：在 UI 上或通过 API 为 v1.3 或 v1.4 生成 JSON 格式的 SBOM 报告，并尝试通过 /api/projects/{projectId}/versions/{projectVersionId}/reports/{reportId}/contents 检索该报告时，会以非 JSON 格式显示，包括“/n”字符。
- (HUB-37763)。修复了以下问题：许可证管理中的组件计数 API 与链接的“使用位置”计数结果不匹配。

- (HUB-37796)。修复了以下问题：MaaS 可能会遇到扫描失败，并显示错误“创建或更新代码位置失败”。
- (HUB-37922)。修复了尝试在指定了 100 个以上组件的 BOM 上使用批量操作功能时的一个问题。
- (HUB-38146)。修复了以下问题：包含正斜杠字符 (/) 的项目版本名称以往会导致在报告生成中创建子文件夹。正斜杠字符现在将被替换为下划线字符 (_)。
- (HUB-38347)。修复了以下问题：特征扫描工具在执行 Docker 映像检查器扫描时，没有正确计算源代码的大小，这会导致扫描失败。
- (HUB-38480)。修复了以下问题：无论使用何种排序选项，API 请求 /api/projects 始终会按名称排序。
- (HUB-38535)。修复了以下问题：/api/components/<component ID>/versions/<version ID>/licenses/<license ID> API 请求在更改后不会返回正确的许可证审批状态。
- (HUB-38554)。修复了以下问题：在使用 HUB UI 浏览 KB 组件版本时，无论用户指定的条目如何，它都会将分页强制设置为 25。
- (HUB-38587)。修复了以下问题：kbMatchTimeoutProperty 被意外设置为硬编码值 (100000ms)；而正确操作是：应该始终从 blackduck-config.env 文件中读取它。
- (HUB-38590)。修复了以下问题：“添加组件”对话框的“所有来源”下拉列表仅显示 10 行，这可能会导致某些来源无法显示。
- (HUB-38598)。修复了以下问题：“组件经理”角色在创建后尝试访问自定义组件版本时可能会出现“403 禁止”错误。
- (HUB-38646)。修复了私有存储库通过 SCM 集成不可见的问题。请注意，您可能需要从 Black Duck 中删除现有令牌，以使这些更改生效。
- (HUB-38679)。在“组件”报告中，将“需要履行”列重命名为“组件版本状态”，因为该报告包含组件版本的“审批状态”以提高可用性。
- (HUB-38685)。修复了项目自动删除在更新后未使用新设置的问题。
- (HUB-38720)。修复了许可证文本区域太小的问题。
- (HUB-38774)。修复了以下问题：如果某个项目版本不会保留，在尝试取消设置该项目版本中的“发布日期”字段时，先前设置的日期会留在原位。

Black Duck SCA 2023.4.x

Black Duck 版本 2023.4.2

公告

目前尚未发布有关 Black Duck 2023.4.2 的新公告。

新增和更改的功能

Black Duck 2023.4.2 中没有新增或更改的功能。

API 增强

Black Duck 2023.4.2 中没有新增或更改的 API 请求。有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

二进制扫描程序信息

Black Duck 2023.4.2 中的二进制扫描程序没有更改。

已修复的问题

在此发布中修复了客户报告的以下问题：

- (HUB-25500)。为在 AWS 上运行的用户添加了机制，以启用此问题的解决方案。如果用户发现上传缓存服务的 CPU 使用率很高，我们鼓励遇到此问题的用户联系 Black Duck 支持部门。此问题将在即将发布的 Black Duck 2023.10.0 版本中修复。
- (HUB-38587)。修复了 kbMatchTimeoutProperty 被意外设置为硬编码值 (100000ms) 的问题。现在，软件将按照预期从 blackduck-config.env 文件中读取它。
- (HUB-38735)。修复了以下问题：在使用 PostgreSQL 容器时，从基于 PostgreSQL 9.6 或 PostgreSQL 11 的 Black Duck 版本升级到 Black Duck 2023.4.1 可能会导致 postgres-upgrader 失败并且无法启动应用程序。
- (HUB-38815)。修复了 Black Duck 快速扫描中可能导致扫描失败的间歇性 ResourceAccessException 错误。

Black Duck 版本 2023.4.1

公告

对存储和注册的节点限制

使用 Black Duck 2023.4.1 后，系统会提醒具有多节点群部署的用户检查对存储和注册的节点限制。此更改将有助于缓解容器移动节点和跨多个系统分布数据。

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

新增和更改的功能

改进了未匹配的文件数据清除

现在，您可以清除专门处于“已存档”项目阶段的项目版本的未匹配文件数据。可以通过“管理”>“系统设置”>“数据保留”页面以全局方式完成此操作，这将影响所有项目；也可以在选定项目的“设置”页面上以本地方式针对该项目完成此操作。

请注意，全局设置仅适用于未明确指定其自身设置的项目和扫描；同样，更改全局设置不会影响指定了其自身设置的项目或扫描。

根据策略进行 SBOM 报告验证

现在，您可以配置特定的项目组，以根据策略验证 SBOM 报告的生成。

这是项目组级别的一项新设置（具有项目组访问权限），可以启用该设置，以防止在具有任何策略违反的项目中生成 SBOM 报告，并提供将该设置应用于组中的项目或所有子组中的所有项目的功能。

在启用该设置后，在尝试生成 SBOM 报告时，系统将通知您无法生成报告，因为项目存在策略违反。

针对 SBOM 报告的新 SPDX v2.3 支持

您现在可以用 SPDX v2.3 格式导出项目的软件材料清单报告。

新的“项目别名 SBOM”字段

添加了一个新的可选“项目别名 SBOM”字段，用于在项目级别覆盖项目名称和版本信息字段。您必须先在“管理”>“SBOM”>“项目”下激活该字段。在启用该字段后，您可以在项目页面 >“设置”下更改项目的别名。

API 增强

更新了扫描端点 BDIO 标头信息

以下 API 端点已更新为使用 BDIO 标头中的项目和版本名称，而不是使用 HTTP 标头中的项目和版本名称：

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

二进制扫描程序信息

已修复的问题

在此发布中修复了客户报告的以下问题：

- (HUB-33736)。更新了多个 API 端点，以使用 BDIO 标头中的项目和版本名称，而不是使用 HTTP 标头中的项目和版本名称。有关更多详细信息，请参阅 API 增强功能部分。
- (HUB-36776)。修复了以下问题：在“来源”选项卡中为组件选择“在文件树中显示”，不会在二进制扫描的文件部分的左侧文件树中显示文件。
- (HUB-37280)。修复了 SPDX 2.2 中的以下问题：即便将“filesAnalyzed”设置为 false，仍会列出所有项目文件。
- (HUB-38005)。从“查找”>“组件”页面中移除了“已报告的漏洞”排序选项，因为不再支持该选项。
- (HUB-38141)。修复了一个争用条件：当扫描客户端请求的源文件不属于任何匹配的目录/存档，并且这些源文件未存储在数据库中时，可能会导致代码段扫描结果不一致。
- (HUB-38212)。修复了以下问题：在导入 CycloneDX 报告时，可能会发生空指针异常错误。
- (HUB-38244)。修复了以下问题：Detect 在代理后运行时，如果与 SIG Artifactory 通信，Detect 配置页面可能会显示错误消息。
- (HUB-38279)。修复了 Black Duck UI 中“仪表板”选项卡下的以下问题：“导出当前视图”按钮未导出“保存的搜索”的当前视图。
- (HUB-38312)。修复了以下问题：“子项目”中批量忽略组件的漏洞更改未累积到父项目。

- (HUB-38328)。修复了以下问题：由于 i18n 字符不正确而未在日语设置中正确显示策略覆盖日期信息。

Black Duck 版本 2023.4.0

公告

为 Azure PostgreSQL 用户升级到 2023.4.0

如果您使用 Azure PostgreSQL 进行升级或安装，则在安装或升级到 2023.4.0 或更高版本之前，数据库管理员需要启用 hstore PostgreSQL 扩展程序的安装。

已将 pgcrypto 扩展程序移动到 st 架构中

从 Black Duck 2023.4.0 开始，将 pgcypto PostgreSQL 扩展程序从公共架构移动到 st 架构中。如果要使用外部 PostgreSQL 实例进行升级，并且 blackduck 数据库用户不是超级用户，则需要使用以下命令手动重定位扩展程序：

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

在所有其他情况下，移动将自动执行。

移除了 jobrunner 中使用的 MAX_CONCURRENT_JOBS

MAX_CONCURRENT_JOBS 在 Black Duck 2022.10.x 中已弃用，并在此版本中已移除。请参阅 Swarm 和 Kubernetes 安装指南，以获得配置较新机制的帮助。

在启用 MaaS 的系统中弃用 KBMATCH_SENDPATH

Black Duck 2023.4.0 现在正式推出“匹配即服务”(MaaS) 功能，默认情况下为新客户启用此功能，此功能将成为所有现有客户的标准配置。作为此更新的结果，在即将发布的 Black Duck 版本中，禁用将文件路径元数据发送到 KnowledgeBase 以进行匹配的选项 (KBMATCH_SENDPATH) 将被移除。

想要继续使用此选项的客户将需要联系 Black Duck 支持部门，以便为其 Black Duck 注册密钥禁用 MaaS。

Docker 18.09.x 和 19.03.x 支持即将结束

从 2023.7.0 版本开始，Black Duck 将不再支持 Docker 18.09.x 和 19.03.x。Docker 20.10.x 将是唯一支持的版本。

Black Duckctl 的生命周期即将结束

从 2023.7.0 版本开始，将不再支持 Black Duckctl，并且不再提供更新。Black Duckctl 的文档可在 https://github.com/blackducksoftware/hub/tree/master/kubernetes/blackduck 找到。

即将推出的容器扫描硬件要求

使用 Black Duck 2023.10.0 时，需要使用 BDBA 容器来执行容器扫描。这意味着，当前在 Black Duck 中执行容器扫描、但未在其 Black Duck 实例中部署 BDBA 的客户将需要根据我们的 2023.10.0 版本指南分配额外的硬件资源，以利用新的容器扫描功能。

容器扫描的现有功能不会作为此更改的一部分被移除。

文档本地化

2023.1.0 版本的 UI、联机帮助和发行说明已本地化为日语和简体中文。

新增和更改的功能

新的 SBOM 上传功能

Black Duck 中的“扫描”页面已更新，以分离上传报告时接受的可能文件类型。单击“上传文件”按钮时，您可以从 BDIO 扫描、SBOM-SPDX 和 SBOM-CycloneDX 中进行选择。

新的 BOM 匹配分数功能

当我们运行特征扫描时，有时匹配的内容会出现歧义。我们可能会匹配特定的组件和版本，但也有多个其他组件和版本可以匹配。

2023.4.0 中的新增功能：您的项目版本的 BOM 将显示一个包含组件的匹配分数的新列。匹配分数越高，我们就越能确信，匹配的组件实际上就是我们认为的组件和版本。

您可以在“管理”>“系统设置”>“组件匹配分数”中配置如何计算匹配分数阈值。通过配置您的匹配分数阈值，您可以减少模糊匹配和低百分比匹配，从而减少在匹配结果中显示的误报。请注意，将阈值配置得太高可能会导致在匹配结果中丢失正报。

由于通过新的匹配模糊逻辑实现了改进，您在查看 BOM 时可能会看到不同的结果。

新的集中式 Black Duck Detect 托管和版本管理

Black Duck 现在提供了一种新的 Black Duck Detect 连接方式，以更好地满足您的需求；Black Duck 托管。此方法最适合希望 Blackduck 管理要使用的 Detect 版本的非物理隔离客户。在系统设置中，Black Duck 将提供主要 Detect 版本及其最新确切版本的下拉列表，您可以从中选择版本以执行扫描。

新的 Artifactory 集成功能

Black Duck 2023.4.0 现在允许使用 JFrog Artifactory 的 Kubernetes 用户对其工件执行二进制和 Docker 映像/容器扫描，从而扩展早期阶段支持的特征扫描。目前，我们支持两种部署选项：完整本地部署和混合部署。有关部署要求和说明，请参阅 Kubernetes 安装指南。

所有扫描入口端点上的新扫描速率限制

基于堆内存，如果扫描容器使用的可用已分配堆 (HUB_MAX_MEMORY) 超过 80%，
它会等到堆使用率达到 60% 后再允许再次扫描。容器还允许每 300 秒扫描一次（这是 blackduck.scan.ingress.scanPassThroughIntervalSecs 的默认值），即使速率限制已启用并处于活动状态，也是如此。

新的 Black Duck 存储容器

Black Duck 2023.1.0 添加了一项新的存储服务，使您能够将静态文件（如 SBOM 和其他报告）移动到持久存储，从而释放数据库并增强扫描性能和可扩展性。

注意：Black Duck 2023.1.0 发行说明中意外遗漏了此项目。

Blackduck 存储的自定义卷的新配置

从 2023.4.0 开始，存储容器可配置为最多使用三 (3) 个卷来存储基于文件的对象。此外，可以将配置设置为将对象从一个卷迁移到另一个卷。备份脚本 hub_create_data_dump.sh 和 hub_db_migrate.sh 已更新，以相应地保存文件提供程序卷。

新的热图过滤支持

您现在可以过滤热图中显示的数据。过滤选项包括代码位置 ID、代码位置名称、项目名称、扫描数据、扫描状态、扫描类型和版本名称。

增强了用于 BOM 支持的快速扫描结果数据

您现在可以配置快速扫描以提供完整的结果格式，以包括用于 BOM 支持的数据点。为此，请设置以下环境变量：BLACKDUCK_RAPID_SCAN_EXTENDED_DATA=true。新数据点包括：

- componentDescription
- 主页链接
- OpenHub 链接
- 声明的许可证定义
- 发布日期
- 指向组件 ID、组件版本 ID 和组件版本来源 URI 的元链接
- 外部命名空间
- 软件包 URL
- SPDX 许可证 ID
- 来源（NVD 或 BDSA）
- 匹配类型

增强的策略违反管理

现在，您可以在 Black Duck BOM 页面上为策略覆盖设置到期日期。通过单击组件的违反图标，可以输入覆盖策略违反的截止日期。当它到期时，它将返回到违反状态。

增强的依赖关系树视图

现在，您可以在依赖关系树视图中突出显示所需的信息，以便复制/粘贴该信息。

移除了 Detect Desktop 的 CentOS 下载链接

“工具”页面已更新，移除了 Detect Desktop 的 CentOS 下载链接，因为 Black Duck 不再支持该链接。

针对 PostgreSQL 15 的初步支持

Black Duck 2023.4.0 增加了对使用 PostgreSQL 15 作为外部数据库的初步支持。此支持仅用于测试；不支持生产用途。

支持的浏览器版本

- Safari 版本 16.3（17614.3.7.1.7、17614）
  - 不再支持 Safari 版本 13.1 和更低版本
- Chrome 版本 111.0.5563.146（正式版本）(x86_64)
  - 不再支持 Chrome 版本 79 和更低版本
- Firefox 版本 111.0.1（64 位）
  - 不再支持 Firefox 版本 74 和更低版本
- Microsoft Edge 版本 111.0.1661.62（正式版本）（64 位）
  - 不再支持 Microsoft Edge 79 和更低版本

容器版本

- 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 增强

更新了组件端点

以下公共 API 端点已更新，以允许更新组件、版本和来源 ID。

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

新的 JobHistoryAppService API 端点

添加了两个新的公共 REST API 端点，它们使用 JobRuntimeRepository 获取有关作业运行时的信息并提供有关它们的信息：

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

新的 JobRuntimeAppService API 端点

添加了两个新的公共 REST API 端点，它们使用 JobRuntimeRepository 获取有关作业运行时的信息并提供有关它们的信息：

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

请注意，您应使用 /api/job-runtimes 端点查看正在运行的作业。现有 /api/jobs 端点将被弃用，以支持新端点。

新的 JobScheduleAppService API 端点

添加了三个新的公共 REST API 端点，它们可输出在系统上计划的作业列表。

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

请注意，您应使用 /api/job-schedules 端点查看计划的作业。现有 /api/jobs 端点将被弃用，以支持新端点。

新的 JobRunner API 端点

添加了一个新的公共 REST API 端点，允许用户启用/禁用定期作业。请注意，以这种方式更改设置可能会导致系统出现意外行为。

- /api/jobs-schedules-configurations

新的集中式 Detect 版本管理 API 端点

已添加以下端点，以支持 Black Duck 2023.4.0 中提供的全新集中式 Detect 版本管理功能：

- GET /api/settings/detect
  - 获取当前的 Detect 版本管理设置
  - 如果由经过身份验证的非系统管理员用户访问，则他们只能接收 detectUri（如果具有值）
  - 如果由经过身份验证的系统管理员用户访问，他们将收到以下信息：
    - detectUri：系统管理员保存的 Detect URI。
    - useInternalHosting：布尔值，确定用于 Detect 的托管类型（内部托管或 Black Duck 托管）。如果未使用内部托管版本的 Detect，则返回 false。
    - useMajorVersion：布尔值，确定是否使用 Detect 主要版本的最新版本。如果在 UI 中选择了 “最新 8.x” 或 “最新 7.x” ，则返回 true。
    - selectedVersion：字符串，返回所用 Detect 的版本。
    - allowDowngrade：布尔值，告知系统设置是否允许用户使用较旧版本的 Detect。
    - majorVersions：字符串，Detect 的当前有效主要版本的列表。
    - allVersions：字符串，Detect 的所有当前有效版本的列表。
- PATCH /api/settings/detect
  - 更新 Detect 版本管理设置
  - 要求由系统管理员用户进行经过身份验证的访问
  - 更新以下信息：
    - detectUri：内部 Detect URI。
    - useInternalHosting：布尔值，设置用于 Detect 的托管类型（内部托管或 Black Duck 托管）。
    - useMajorVersion：布尔值，设置 Detect 的最新主要版本或显式版本。已更新，如果 useInternalHosting 为 false，则为必填项。

- selectedVersion：字符串，要使用的 Detect 版本（主要版本或确切版本）。仅在 useInternalHosting 为 false 时更新。
- allowDowngrade：布尔值，如果受管，则允许使用早期版本的 Detect。

弃用 PUT /api/settings/data-retention

如 2022.10.0 发行说明中所述，已弃用 PUT /api/settings/data-retention 并替换为 PATCH /api/settings/data-retention。在 Black Duck 2023.4.0 中，PUT /api/settings/data-retention 现在将返回 HTTP 405 METHOD_NOT_ALLOWED 错误消息。

二进制扫描程序信息

二进制扫描程序已更新为版本 2023.3.0。

。

已修复的问题

在此发布中修复了客户报告的以下问题：

- (HUB-32471)。修复了以下问题：当扫描存在 KnowledgeBase 连接问题时，UI 中未报告问题并导致 BOM 为空。
- (HUB-33018)。修复了打印 BOM 时可能出现垂直和水平滚动条的问题。
- (HUB-34474)。修复了以下问题：当项目名称包含全角大写字母时，过滤项目无法正确显示。
- (HUB-34616)。修复了以下问题：“诊断”页面上列出的作业不显示已完成作业的毫秒数。
- (HUB-34964)。修复了以下问题：“查找”页面上的漏洞“使用者”计数与受漏洞影响的项目页面不一致。
- (HUB-34981)。修复了以下问题：组件版本列表视图上的“使用者”计数与组件版本详细信息视图不一致。
- (HUB-35075)。修复了在 Chrome 浏览器中尝试将 BOM 页面保存为 PDF 时的显示问题。
- （HUB-35092、HUB-35171、HUB-36088）。修复了以下问题：使用 API 请求在存档阶段向项目/版本添加或删除组件会导致返回 200 OK 响应，但实际上并未添加或删除该组件。现在，如果尝试执行此操作，将显示一个错误。UI 也将不再显示“删除”选项。
- （HUB-35773、HUB-37305）。修复了以下问题：由于二进制扫描，在 BOM 的“源”选项卡中，与多个组件匹配的单个文件将仅显示其中一个组件。
- (HUB-35836)。修复了以下问题：从项目中移除项目所有者时，Black Duck 未阻止项目成为孤立项目。现在添加了直接访问用户分配检查，以防止执行此操作。
- (HUB-36108)。修复了由于 QuartzSnippetScanAutoBomJob 而导致的代码段扫描长时间运行和超时问题。
- (HUB-36351)。修复了有关更新自定义组件版本和创建自定义组件版本的 API 文档。
- (HUB-36387)。修复了修复状态更新中的并发问题：通过 API 缓解特定漏洞将允许应用缓解措施，但 riskPriorityDistribution 不反映所有缓解措施。
- (HUB-36446)。修复了下载 Sigma 工具可能失败并显示 HTTP 401 未授权消息的问题。
- (HUB-36676)。修复了尝试在 OpenShift 环境中安装 Platform One Black Duck 时的文件权限问题。
- (HUB-36716)。修复了以下问题：BDSA 自动修复的漏洞不会从新项目版本或克隆项目中的已忽略组件中移除。

- (HUB-36719)。修复了以下问题：将子项目添加到父项目时，即使取消选中“包括在通知文件报告中”复选框，在通知报告中仍然会包括子项目的信息。取消选中主题的此复选框现在将从项目层次结构内的上方所有项目中排除子项目。
- (HUB-36763)。修复了 SigmaToolStoreStateCheckAndRetryJob 可能因用户配置的代理而失败的问题。如果不使用代理时无法访问 sig-repo，但使用代理时可以访问 sig-repo，则作业将不再失败。
- (HUB-36905)。修复了以下问题：对单个叶文件进行特征扫描会导致出现空指针异常错误。
- (HUB-36952)。修复了文件和软件包调整操作中的空指针异常。
- (HUB-37031)。修复了启用 MaaS 时匹配计数差异和匹配文件响应中缺少 URI 属性的问题。
- (HUB-37078)。修复了多个 UI 页面上的问题：浏览器中的“后退”按钮可能需要多次尝试才能正常工作。
- (HUB-37109)。移除了在代码段匹配上设置用途的功能，因为该产品当前不支持该功能。它仍可用于所有其他匹配类型。
- (HUB-37232)。修复了以下问题：在上传源代码后打开“发现”时自动滚动功能有时不起作用：许可证、许可参考、版权。
- (HUB-37233)。修复了 REST API 文档的问题：“请求的 BOM 组件展示的特定子集”的描述中的“BOM 组件展示”链接将转至“BOM 组件版本展示”，而不是“BOM 组件展示”。
- (HUB-37308)。修复了以下问题：“扫描”页面列表中的扫描大小包括代码段扫描大小，因而错误地显示两者的大小之和。
- (HUB-37312)。修复了以下问题：查找对象时，如果挂载的存储卷中不存在 /opt/blackduck/hub/uploads/tools 目录，则会生成“无法访问工具”错误。
- (HUB-37414)。修复了以下问题：“项目 BOM”页面上的扫描状态可能会停留在“处理中”状态，只有通过刷新页面才能更新状态。
- (HUB-37439)。修复了以下问题：代码段匹配的路径长度过长，导致在代码段视图中无法完全显示路径。
- (HUB-37453)。修复了以下问题：在项目版本页面上应用任何过滤器后，然后刷新页面或离开页面时，不会保存所应用的过滤器设置。
- (HUB-37505)。修复了“作业”页面 (/api/jobs) 上的作业顺序不正确的问题。现在将按结束时间降序列出作业。
- (HUB-37554)。修复了以下问题：使用 /api/projects/<id>/versions/<id>/components/<id>/versions/<id> API 请求时，如果缺少 component 和 componentVersion 参数，可能会导致错误。要将组件设置为未知版本，请将 componentVersion 字段设置为空字符串 ""。
- (HUB-37648)。修复了二进制扫描（集成了 BDBA）的问题：即使“组件”选项卡和“组件”报告显示多个组件，“来源”选项卡和“来源”报告也只显示每个二进制文件的单个组件匹配。
- (HUB-37661)。修复了以下问题：当 BOM 引用另一个项目时，“安全”选项卡显示空白加载区域。
- (HUB-37696)。修复了以下问题：包含组件 URL 的注释无法正确换行，导致其超出屏幕。出于安全原因，链接将显示为纯文本。用户需要复制粘贴才能导航到它们。
- (HUB-37757)。修复了以下问题：由于在使用后页面未按预期刷新，“扫描”页面上的“删除”按钮在使用后会停止工作。
- (HUB-37775)。修复了以下问题：尝试使用编辑选项手动添加组件来源时，无法完全显示来源 ID 的完整路径。
- (HUB-37789)。修复了无法再从来源树视图复制匹配文件/文件夹名称的问题。
- (HUB-37925)。修复了通过“摘要”选项卡上的选项过滤项目后无法通过 UI 移除过滤器的问题。

Black Duck SCA 2023.1.x

Black Duck 版本 2023.1.2

公告

更新了自动项目版本删除功能

Black Duck 2023.1.0 更新了自动项目版本删除功能（以前称为自动数据移除）。现在，在升级到 2023.1.0 和任何即将发布的将来版本时，默认情况下会启用此功能。

自动项目版本删除允许自动移除 Black Duck 中的旧项目版本。默认设置将移除 90 天内未更新或扫描的项目版本。升级到 2023.1.x 后，如果在 45 天内未更新或重新扫描旧项目版本，该版本将在升级 45 天后删除，前提是这些版本在升级后未重新扫描或更新。可以在系统管理员数据保留设置页面中更改这些设置。

新增和更改的功能

新的自动 OAuth 令牌刷新

Black Duck 现在将在 GitLab 和 Bitbucket 访问令牌过期后自动重新生成它们。

增强的热图功能

处于“已启动”状态的扫描现在将包含在热图 UI 指标中。

API 增强

Black Duck 2023.1.2 中没有新增或更改的 API 请求。有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

二进制扫描程序信息

Black Duck 2023.1.2 中针对二进制扫描程序没有新增或更改的功能。

已修复的问题

在此发布中修复了客户报告的以下问题：

- (HUB-35747)。修复了阻止某些定期作业（BomAggregatePurgeOrphansJob、KbUpdateWorkflowJob）完成的问题。
- (HUB-36781)。修复了以下问题：在 Kubernetes 或 OpenShift 上无法使用自定义 fsGroup 安装 Black Duck 2022.10.x 版本。
- (HUB-36796)。已修复一个问题，其中，将用户直接分配给项目组，并将同一用户分配给也分配给项目组的用户组时，将导致 API 返回多个项目组，从而导致 Detect 失败。
- (HUB-36939)。修复了以下问题：如果用户以 sysadmin 身份登录 Black Duck，调试页面会以纯文本格式显示密码。

- (HUB-36997)。修复了以下问题：使用本地 KnowledgeBase 生成的通知文件缺少许可证信息。
- (HUB-37143)。修复了以下问题：如果组件没有版本，则用于评估策略表达式“较新版本计数”的快速扫描会因内部错误而失败。
- (HUB-37285)。修复了以下问题：如果更改默认管理员用户名，使用外部数据库的 Black Duck 2023.1.0 的新安装可能会失败。
- (HUB-37312)。修复了以下问题：查找对象时，如果挂载的存储卷中不存在 /opt/blackduck/hub/uploads/tools 目录，则会生成 Unable to access tool 错误。

Black Duck 版本 2023.1.1

公告

目前尚未发布有关 Black Duck 2023.1.1 的新公告。

新增和更改的功能

Black Duck 2023.1.1 中没有新增或更改的功能。

API 增强

Black Duck 2023.1.1 中没有新增或更改的 API 请求。有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

二进制扫描程序信息

二进制扫描程序已更新至版本 2022.12.0，其中包括新的重试策略和修复，以提高与 Black Duck 的网络通信恢复能力，适应扫描容量资源限制的扩展，从而确保集成式二进制扫描的可靠性。

已修复的问题

此版本修复了以下问题：

- (HUB-37171)。修复了启用加密时身份验证容器无法联机的问题。

Black Duck 版本 2023.1.0

新增和更改的功能

已更新 SCM 集成 - 阶段 3

Black Duck 2023.1.0 在 SCM 集成列表中添加了两个新的 SCM 提供商：

- GitLab Self-Managed
- Bitbucket Data Center

现在，您可以添加这些授权的 SCM 提供商，然后在创建新项目时选择这些提供商。这样做之后，将自动在新项目的“项目设置”页面中预填充存储库 URL 和分支版本。

此功能与 Detect 8.x 及更高版本兼容，并将在新的软件包管理器扫描中生效。

请注意，在 Black Duck 中默认情况下不启用 SCM 集成，必须通过在您的环境中添加以下内容来激活此功能：

对于 Swarm 用户，请将以下内容添加到您的 blackduck-config.env 文件中：

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

对于 Kubernetes 用户，请将以下内容添加到您的 values.yaml 文件中的 environs 部分下：

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

更新了项目版本自动删除

项目版本自动删除（以前称为自动数据移除）现在在 Black Duck 用户界面中进行管理。为此，请单击“管理”>“系统设置”>“数据保留”。

在特征扫描处理过程中增强了文件大小的分析和聚合

过大的扫描将不再中断匹配引擎服务，而是将使扫描失败，并显示错误，指出计算的大小大于注册的限制。计算的大小为：

- 扫描的完整大小（如果在配准限制范围内）。
- 上次计算的扫描大小（在扫描超出注册限制后）。如果扫描大小已超出许可限制，则不会计算扫描大小。

无状态特征扫描（以前称为临时特征扫描）

无状态扫描是一种新的扫描模式，它不会在 Black Duck 中创建或使用任何永久存储，因此不会存储材料清单 (BOM)。它用于快速查找指定扫描目标内的策略违反。要使用无状态扫描，您必须具备以下组件：

- Black Duck Detect 8.2.0 或更高版本
- Black Duck 2022.10.0 或更高版本
- 托管知识库
- 必须启用“匹配即服务”

增加了对 Docker Swarm 密钥加密的支持

Black Duck 增加了对 Docker Swarm 密钥加密的支持，以集中管理数据（如密码、SSH 私钥、SSL 证书或其他数据），并仅将其安全地传输到需要访问数据的容器。

增加了应用程序级加密和密钥轮换

从版本 2023.1.0 开始，Blackduck 支持在系统中加密关键数据，例如 Git SCM Oauth 令牌、Git 应用程序密钥、SAML 私有特征密钥和 LDAP 凭据。此加密基于编排环境（Docker Swarm 或 Kubernetes）调配给 Blackduck 安装的密钥。

新的“组件见解”页面

扫描中发现的某些组件可能具有附加详细信息，有助于确定组件来源的额外信息。“组件见解”页面可让您更好地了解组件的运行方式以及提供的功能。如果组件具有附加见解，您可以通过转到项目版本的页面，然后在该组件的选项菜单中选择“见解”进行查看。

项目组的新 SBOM 报告字段

现在，您可以向项目组添加新的附加 SBOM 字段，以便在软件材料清单 (SBOM) 报告中包含更多详细信息：

- 创建者：创建 SPDX 文件的人员或组织，包括电子邮件地址。
- 创建者备注：SPDX 文件创建者的可选字段，用于提供有关 SPDX 文件创建的一般备注或其他字段中未包含的任何其他相关备注。

新的 KB 许可证更新和安全更新作业

当前 KB 更新作业将拆分为 KB 安全更新作业和 KB 许可证更新作业。默认情况下，KB 许可证更新作业计划为每天运行，可进行配置以更改作业频率，并允许您在需要时使用以下系统属性禁用作业：

- KB_LICENSE_UPDATER_PERIOD_MINUTES：以分钟为单位设置作业频率。
- KB_UPDATE_JOB_ENABLED：设置为 false 可禁用安全和许可证更新作业。

更新了 SBOM 报告中的 referenceLocator URL

SBOM 报告中的 referenceLocator 字段现在将仅显示 Black Duck KB 唯一 ID，而不是 URL。

增强了快速扫描功能

Black Duck 2021.10.0 引入了项目组定义的策略规则，以便客户可以按特定项目组确定策略规则的范围（只能在完整扫描模式下使用）。Black Duck 2023.1.0 中的新增功能：基于项目组的策略现在在“快速扫描”模式下受支持。

Rapid Scan 用户可以使用以下 Detect 参数指定扫描项目的父项目组：

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

- 项目组名称必须与 Black Duck 上的现有项目组完全匹配。
- 如果提供了 <project group name>，而该项目在 Black Duck 中不存在，它将用作策略确定的项目组。

更新了 v3 特征扫描故障处理

从 2023.1.0 开始，所有超出代码位置限制或总扫描代码限制的 v3 特征扫描都将在创建时失败，而不是在进入后失败。失败将不会显示在 Black Duck UI 中，而是显示在扫描客户端上。

改进了与搜索相关的性能

Black Duck 中的搜索使用数据库中定期刷新的具体化视图，以实现更快的搜索结果。但是，刷新这些视图会导致大型数据库出现问题。我们分析了所有过滤器，并确定不需要某些过滤器。从各种搜索类别中，我们移除了以下过滤器：

项目版本搜索

- 分发
- 层级

组件搜索

- 策略规则
- 策略违反严重性
- 组件审批状态
- 审核状态
- 漏洞已报告
- 漏洞 CWE

漏洞搜索

- 基本分数
- 可利用性子分数
- 影响子分数
- 暂时子分数
- 可到达

保存的搜索将通过迁移脚本更新，以移除这些过滤器。添加了书签的搜索结果仍然有效。但是，移除的过滤器将被忽略，因此结果将如同从未选择过该过滤器一样。仅包含已移除过滤器的已保存搜索将被完全移除。

新的扫描热图

现在，您可以查看按需热图，该热图显示过去 30 天内给定日期和小时执行的扫描总数。彩色编码矩阵显示基于最小/最大关系的扫描总数，绿色值表示较低值，红色值表示较高值。通过单击“管理”按钮，然后在“诊断”部分中选择“热图”，可以在 Black Duck 中找到热图。

新的 Black Duck 存储容器

Black Duck 2023.1.0 引入了一项新的存储服务，使您能够将静态文件（如 SBOM 和其他报告）移动到持久存储，从而释放数据库并增强扫描性能和可扩展性。

报告模式更改

在 Black Duck 2023.1.0 中，reporting.scan_view 中 basedir 列的类型已从字符变化更改为文本，以容纳长度超过 255 个字符的路径。

新的“项目组管理员”角色

新的“项目组管理员”角色能够在本地级别管理项目组。例如，他们能够创建/编辑/删除项目组，并从其父项目组下的项目组中添加/移除成员和用户组。

支持的浏览器版本

- Safari 版本 16.2（17614.3.7.1.7，17614）
  - 不再支持 Safari 13.0 和更低版本
- Chrome 版本 109.0.5414.87（正式版本）(x86_64)
  - 不再支持 Chrome 版本 71 和更低版本
- Firefox 版本 109.0（64 位）
  - 不再支持 Firefox 版本 71 和更低版本
- Microsoft Edge 版本 109.0.1518.55（正式版本）（64 位）

- 不再支持 Microsoft Edge 版本 78 和更低版本

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

增强了项目端点

以下端点已更新为包括 OSS 组件 pURL 坐标：

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

更新了数据保留 API 端点

以下端点已从 PUT 更改为 PATCH 请求：

- /api/settings/data-retention

新工具列表 API 端点

现在有一个新的公共端点可用于列出所有可用的工具版本：

- /api/tools

针对特定项目组获取 SBOM 字段

现在，可以使用新的公共端点来读取项目的 SBOM 字段：

- /api/project-groups/{projectGroupId}/sbom-fields

二进制扫描程序信息

二进制扫描程序已更新至版本 2022.12.0，其中包括新的重试策略和修复，以提高与 Black Duck 的网络通信恢复能力，适应扫描容量资源限制的扩展，从而确保集成式二进制扫描的可靠性。

已修复的问题

在此发布中修复了客户报告的以下问题：

- (HUB-32387)。修复了 Redis 无法在默认 OpenShift 环境中访问 /data 的问题。
- (HUB-33820)。修复了以下问题：在 BOM 中更新组件后会出现警告（例如，该组件在 KnowledgeBase 中的状态设置为“已审查”），但在用户手动重新加载页面之前该警告不会消失。
- (HUB-34056)。修复了以下问题：在“编辑”对话框中选中“调整代码段并确认”时，单个组件编辑显示的结果与批量组件编辑不同。
- (HUB-34374)。修复了以下问题：项目版本页面的“来源”选项卡上的“发现类型”列中的值在使用过滤器时显示不一致。
- (HUB-34502)。修复了以下问题：在报告中包含忽略的组件时，已确认/未确认的代码段结果未包含在源报告中。
- (HUB-34596)。修复了以下问题：尝试创建与内部用户共享相同用户名的 SAML 用户时出现重复限制错误。
- (HUB-34725)。修复了版本报告中重复的 FILE_DEPENDENCY_DIRECT 和 FILE_DEPENDENCY_TRANSITIVE 条目的问题。
- (HUB-34756)。修复了以下问题：使用 API 通过项目组分配用户组角色时，范围显示为“服务器”。
- (HUB-34947)。修复了以下问题：SPDX 报告中可能显示忽略的代码段。
- (HUB-35472)。修复了以下问题：在 synopsysctl 中更改 MAX_TOTAL_SOURCE_SIZE_MB 的值没有正确应用。
- (HUB-35557)。修复了以下问题：格式不正确的 /api/projects/ 请求将返回 HTTP 5xx 错误代码而不是返回 HTTP 4xx 错误代码。
- (HUB-35585)。修复了以下问题：“更新者”数据未更新，始终将“系统管理员”显示为进行更改的用户的用户名且具有旧日期/时间。
- (HUB-35764)。修复了顶部菜单和代码段窗口中的一些 GUI 错误。
- (HUB-35912)。修复了以下问题：应用包含所有选定选项的许可证风险过滤器时，已确认然后忽略的代码段匹配会消失。
- (HUB-35914)。修复了 system_check.sh 脚本中的错误标志（使用 -z，而不是 -n）。
- (HUB-35927)。修复了以下问题：如果组件的 CVE BDSA 映射发生更改，自动修复功能不会恢复修复状态和注释。
- (HUB-35945)。修复了以下问题：项目版本的“扫描”页面上的“扫描大小”值不包括主“扫描”页面上显示的代码位置的大小值。
- (HUB-36321)。修复了以下问题：“项目查看者”角色可以使用代码段的“来源”视图中的“编辑”选项。
- (HUB-36382)。修复了在快速连续接收多个扫描时生成错误的罕见争用条件。

- (HUB-36498)。修复了以下问题：如果 CVE 记录过多，GET /api/vulnerabilities/<CVE RECORD>/affected-projects 会返回 HTTP 400 错误代码。
- (HUB-36629)。修复了以下问题：快速扫描可能报告违反策略规则的额外漏洞。
- (HUB-36703)。修复了以下问题：Black Duck UI 和 /api/projects/{projectId}/versions/{projectVersionId}/matched-files API 请求中的匹配类型不同。有关详细信息，请参阅上面的 “API 增强” 一节。
- (HUB-36707)。修复了以下问题：如果项目或版本名称拼写错误，快速扫描可能会超时，而不是错误地快速结束。

Black Duck SCA 2022.10.x

Black Duck 版本 2022.10.3

公告

目前尚未发布有关 Black Duck 2022.10.3 的新公告。

新增和更改的功能

Black Duck 2022.10.3 中没有新增或更改的功能。

API 增强

Black Duck 2022.10.3 中没有新增或更改的 API 请求。有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

二进制扫描程序信息

二进制扫描程序已更新到版本 2022.9.2，其中包括针对高严重性 CVE-2022-3602 和 CVE-2022-3786 漏洞的 OpenSSL 3.0.7 升级。

已修复的问题

此版本修复了以下问题：

- (HUB-37171)。修复了启用加密时身份验证容器无法联机的问题。

Black Duck 版本 2022.10.2

公告

目前尚未发布有关 Black Duck 2022.10.2 的新公告。

新增和更改的功能

Black Duck 2022.10.2 中没有新增或更改的功能。

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

增强了项目端点

以下端点已更新为包括 OSS 组件 pURL 坐标：

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

二进制扫描程序信息

二进制扫描程序已更新到版本 2022.9.2，其中包括针对高严重性 CVE-2022-3602 和 CVE-2022-3786 漏洞的 OpenSSL 3.0.7 升级。

已修复的问题

在此发布中修复了客户报告的以下问题：

- (HUB-35377)。修复了以下问题：在审查未确认/已忽略的代码段时，Black Duck 中除“来源”视图之外的任何位置的组件或许可证使用计数中会显示未确认的代码段和已忽略的组件。
- (HUB-35850)。修复了 Redis 无法在默认 OpenShift 环境中访问 /data 的问题。
- (HUB-36049)。修复了以下问题：FileBackedOutputStream 临时文件写入扫描容器下的 /tmp 目录且未清理。
- (HUB-36149)。修复了以下问题：以 PDF 格式打印 BOM 时不包括项目名称和版本名称。

- (HUB-36359)。修复了 Guthub 版本页面上缺少的 blackduck-webui 容器链接。
- (HUB-36495)。修复了联机帮助中的一些过时图像。

Black Duck 版本 2022.10.1

公告

OpenSSL 版本 3.0.0 至 3.0.6 的安全公告

2022 年 11 月 1 日，OpenSSL Project 披露了 OpenSSL 3.0.x 中存在的以下高严重性漏洞。

这两个漏洞的性质都允许在 X.509 证书验证中触发缓冲区溢出，特别是在名称约束检查中。请注意，这种情况发生在证书链签名验证之后，要求 CA 对恶意证书签名，或者要求应用程序在未能构建指向受信任颁发者的路径的情况下继续进行证书验证。

CVE-2022-3602：攻击者可以创建恶意电子邮件地址，以溢出堆栈上由攻击者控制的四个字节。此缓冲区溢出可能导致崩溃（导致拒绝服务）或可能的远程代码执行。

CVE-2022-3786：攻击者可以在证书中创建恶意电子邮件地址，以溢出堆栈上包含 `.' 字符（十进制 46）的任意字节数。此缓冲区溢出可能导致崩溃（导致拒绝服务）。

目前，Black Duck 认为 Black Duck SIG 产品、服务和系统面临的风险有限。在我们已经接触到的风险范畴内，我们已采取了一些缓解措施，以防止有人试图利用漏洞。

二进制扫描程序 (BDBA) 已更新到版本 2022.9.2，其中包括针对高严重性漏洞的 OpenSSL 3.0.7 升级。运行 2022.10.0 且未配备 BDBA 的客户不需要升级。

请继续关注我们的社区页面以获取更多更新内容。

新增和更改的功能

Black Duck 2022.10.1 中没有新增或更改的功能。

容器版本

- 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 增强

Black Duck 2022.10.1 中没有新增或更改的 API 请求。有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

二进制扫描程序信息

二进制扫描程序已更新到版本 2022.9.2，其中包括针对高严重性 CVE-2022-3602 和 CVE-2022-3786 漏洞的 OpenSSL 3.0.7 升级。

已修复的问题

在此发布中修复了客户报告的以下问题：

- (HUB-36290)。更新了 BDBA 工作器以应对 OpenSSL 漏洞。

Black Duck 版本 2022.10.0

2022.10.0 的公告

弃用 PostgreSQL 11

对在 PostgreSQL 11 上运行 Black Duck 的支持已在 2022.10.0 版本结束。从该版本开始，尝试使用 PostgreSQL 11 运行 Black Duck 将会生成错误，且 Black Duck 将无法启动。

PostgreSQL 13 容器迁移

Black Duck 2022.10.0 已将 PostgreSQL 映像从版本 11 迁移到版本 13，并支持从使用 PostgreSQL 9.6 容器（版本 4.2 至 2021.10.x）或 PostgreSQL 11 容器（版本 2022.2.0 至 2022.7.x）的版本进行升级。在安装过程中，blackduck-postgres-upgrader 容器将现有数据库迁移到 PostgreSQL 13，然后在完成后退出。

强烈建议使用非核心 PG 扩展的客户在迁移前卸载这些扩展，并在迁移成功完成后重新安装；否则，迁移可能会失败。

进行复制设置的客户在迁移之前需要遵循 pg_upgrade 文档中的说明。如果没有进行上述的准备工作，迁移可能会成功，但复制设置将会中断。

不使用 Black Duck 提供的 PostgreSQL 映像的客户不会受到影响。

重要提示：开始迁移之前：

- 确保您有额外的 10% 磁盘空间，以避免由于系统目录的数据复制而导致磁盘使用情况出现意外问题。
- 检查根目录空间和卷安装以避免磁盘空间不足，因为这可能导致 Linux 系统中断。

对于 Kubernetes 和 OpenShift 用户：

- 在普通 Kubernetes 上，升级作业的容器将以 root 身份运行。但是，唯一的要求是作业与 PostgreSQL 数据卷的所有者以相同的 UID 运行。
- 在 OpenShift 上，升级作业假定它将使用与 PostgreSQL 数据卷所有者相同的 UID 运行。

对于 Swarm 用户：

- 迁移完全是自动进行的；除了标准的 Black Duck 升级之外，不需要额外的操作。
- blackduck-postgres-upgrader 容器必须以 root 身份运行才能更改上述布局和 UID。
- 随后 Black Duck 重新启动时，blackduck-postgres-upgrader 将确定不需要迁移，并立即退出。

弃用数据库 bds_hub_report

如 Black Duck 2021.10.0 的发行说明中所述，新安装的 Black Duck 将不再创建 bds_hub_report 数据库。我们将在 2022.10.0 中删除 bds_hub_report 数据库。

希望保存 bds_hub_report 数据库的用户可以使用 hub_create_data_dump.sh 脚本转储 bds_hub_report 数据库（如果存在）。

2022 年 11 月 Black Duck KnowledgeBase IP 地址更改通知

2022 年 11 月 14 日这一周内，Black Duck KnowledgeBase https://kb.blackducksoftware.com IP 地址将更改。在 14 日这一周内，我们将更新 DNS 以将流量定向到新的 IP 地址。对于大多数客户，无需采取任何措施。

使用 IP 允许列表与知识库通信的本地客户需要更新其防火墙，让列表中包含这些新 IP 地址。不使用防火墙规则限制流量或不使用 IP 允许列表的客户不会受到影响。

对于使用 IP 地址的客户，允许列表需要添加以下 IP 地址：

NAM（北美）

kb-na.blackducksoftware.com：34.160.126.173

EMEA（欧洲、中东和非洲）

kb-emea.blackducksoftware.com：34.149.112.69

亚太地区（亚太地区、亚洲和中国）

kb-apac.blackducksoftware.com：34.111.46.24

此更改不会影响使用 DNS 解析的大多数客户，因为这将自动处理 IP 地址更新。使用 IP 地址白名单的客户需要将三个新的 IP 地址添加到其白名单中：34.160.126.173、34.149.112.69、34.111.46.24。

下面列出的当前 IP 地址仅供参考：

NAM：35.224.73.200

EMEA：35.242.234.51

APAC：35.220.236.106

我们进行这一更改是为了确保 KB 能保持高可用性和安全性。

如果在服务器迁移后出现疑问或问题，请提交支持案例。

对象存储服务即将实施的系统资源要求

在 Black Duck 2023.1.0 中，部署对象存储服务的最低系统资源要求将提高。对象存储服务将大约需要额外的 1 个 CPU、1GB 内存和 10GB 磁盘空间。请注意，这些要求将在将来的版本中再次更改。

文档本地化

2022.7.0 版本的 UI、联机帮助和发行说明已本地化为日语和简体中文。

2022.10.0 中的新增功能和更改功能

Git 存储库 SCM 集成 - 阶段 2

Black Duck 2022.10.0 更新了用户在创建项目和版本时添加存储库/分支字段的方式。现在，您可以添加授权的 SCM 提供商（目前仅限 GitHub Standard 和 GitHub Enterprise），然后在创建新项目时可以选择这些提供商。这样做之后，将自动在新项目的“项目设置”页面中预填充存储库 URL 和分支版本。

此功能与 Detect 8.x 及更高版本兼容，并将在新的软件包管理器扫描中生效。

请注意，在 Black Duck 中默认情况下不启用 SCM 集成，必须通过在您的环境中添加以下内容来激活此功能：

对于 Swarm 用户，请将以下内容添加到您的 blackduck-config.env 文件中：

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

对于 Kubernetes 用户，请将以下内容添加到您的 values.yaml 文件中的 environs 部分下：

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

项目版本组件的新批量操作

批量更新功能现在支持对项目版本页面上的组件执行以下操作：

1. 忽略/取消忽略组件
2. 设置组件用法类型
3. 标记为已审查/未审查
4. 设置通知文件中的包含/排除

结合使用 UTF8 与 BOM 创建报告

请注意，Black Duck 2022.7.0 中添加了此功能，但在该版本的发行说明中意外忽略了此功能。

Black Duck 2022.7.0 引入了对 UTF8 BOM 字符编码的支持，可在使用非西方字符的客户的报告中使用此编码。要启用此功能，请将以下内容添加到 blackduck-config.env 文件中：

```
USE_CSV_BOM=true
```

新热图数据下载

现在，要审查和分析终端扫描趋势，您可以下载压缩 CSV 格式的热图，并在电子表格程序中将热图创建为透视图。可通过导航至管理 > 诊断 > 系统信息下载此数据。

新的 SBOM 报告字段

现在，您可以向项目添加新的附加 SBOM 字段，以便在软件材料清单 (SBOM) 报告中包含更多详细信息。SBOM 字段包括以下新字段。

在 BOM 组件级别设置：

- 软件包 URL：对于 SPDX 报告中的 referenceCategory: PACKAGE_MANAGER 元素，在 externalRefs 部分中作为 referenceType: purl 列出，对于 CycloneDX 报告，在 components 部分下作为 purl 列出。
- 软件包供应商：对于两种报告类型，均作为 (supplier) 列出。
- CPE：对于 SPDX 报告中的 referenceCategory: SECURITY 元素，在 externalRefs 部分中作为 referenceLocator 列出，对于 CycloneDX 报告，在 components 部分下作为 cpe 列出。

在组件级别设置：

- 说明：对于两种报告类型，均作为 description 列出。
- 发起者：对于 SPDX 报告，在 packages 部分下作为 originator 列出，对于 CycloneDX 报告，在 components 下作为 author 列出。

新的“全局通知查看者”角色

已创建一个新角色，该角色对所有项目具有只读访问权限，并接收所有系统通知，而不考虑用户首选项。

新的通知订阅管理

现在，您可以启用或禁用您的用户接收的通知。您可以通过转到管理 > 系统设置 > 通知来管理这些设置。请注意，具有“全局通知查看者”角色的用户仍将收到系统上的所有通知。

已更新关注项目的通知管理

现在，您可以在“我的设置”页面中管理从其接收通知的观察项目。为此，请单击右上角菜单上您的用户名，单击“已观察项目”，然后选择“已观察项目”选项卡。

已更新通知保留期

通知保留的默认配置值已从 30 天减少到 14 天。这可以通过设置 blackduck-config.env 中的 BLACKDUCK_HUB_NOTIFICATIONS_DELETE_DAYS 变量来修改。

策略的新漏洞条件

在替换并包括远程执行代码 (RCE) 漏洞的策略的“漏洞条件”中添加了一个新的“漏洞标记”类别。创建或编辑策略时，此类别包括以下过滤器选项：

- 零点击远程代码执行：该漏洞可导致远程攻击者在系统中执行代码，而不需要或依赖任何第三方操作。
- 恶意代码已识别：该软件包含恶意代码，如果在您的系统中执行，该代码会产生有害或破坏性的后果。
- 已禁止漏洞详细信息：目前漏洞的技术详细信息处于禁止状态，供应商此时不会发布详细信息。
- 未确认漏洞：漏洞没有基于代码的修复，因为供应商已确定组件的行为是有意的，并且认为不存在漏洞。

在“漏洞更新”报告中添加了新的漏洞标记

“漏洞更新”报告现在将显示漏洞标记（如果适用）。其中包括上面列出的漏洞标记。

列表和表的新导出功能

现在，您可以在以下页面上将列表和表导出到 CSV：

- “仪表板”页面：在仪表板的“结果摘要”部分中找到。
- “查找”页面：在“查找”页面左侧的搜索字段上方找到。
- “扫描”页面：在“扫描”页面左上方的删除按钮旁边找到。
- “用户和组”页面：在“用户和组”页面左上方的“创建用户”按钮旁边找到。

增强了为二进制文件扫描和 Protex BOM 导入导入 BDIO 时来源视图

当前，“扫描”页面在 BOM 导入日志中列出了未找到组件。现在，在 2022.10.0 版本中，未匹配的组件也将出现在“来源视图”选项卡中。请注意，未匹配的组件将仅在新扫描的来源视图中出现。现有扫描将保持不变。

报告模式增强

reporting.component 视图现在有三个附加字段：

- reporting.component.created_at：从 BOM 复制的组件创建时间。表示组件首次添加到 BOM 的时间。

- reporting.component.updated_at：从 BOM 复制的组件更新时间。表示组件在其 BOM 中最近更新的时间。
- reporting.user_group_project_mapping：添加内容以表明哪个用户映射到哪个组、哪个用户映射到哪个项目。

新的临时特征扫描 - 客户可用性受限

Ephemeral Signature Scan 是一种新的扫描模式，它不会在 Black Duck 中创建或使用任何永久存储，因此不会存储材料清单 (BOM)。它用于快速查找指定扫描目标内的策略违反。要使用临时特征扫描，您必须具备以下组件：

- Black Duck Detect 8.2.0 或更高版本
- Black Duck 2022.10.0 或更高版本
- 托管知识库
- 必须启用“匹配即服务”

请注意，此功能具有受限的客户可用性，通常不适用于 Black Duck 2022.10.0。

已更新 synopsysctl

Black Duckctl 已更新，可与新的 PostgreSQL 13 容器一起使用。

容器版本

- 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 增强

有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

新的扫描监控 API 端点

添加了一个新的 REST API 端点，它可分析扫描错误率，并允许您在给定的时间范围内（默认设置为上一小时）从系统中的终端扫描获取扫描监控信息：

- GET /api/scan-monitor

请求参数如下：

- level （必填）。数值 1 或 2，默认值为 1。
  请求示例： GET /api/scan-monitor?level=1

  级别 1 是简单的二进制响应，要么为 OK，要么为 NOT OK（如果故障率超过设置的最大阈值 [默认值为 30%]）。

  级别 2 返回十六进制颜色代码（绿色、黄色或红色），具体取决于状态。绿色 (#00FF00) 表示在监控的时间范围内（默认值为上一小时）的故障率小于设定的最小阈值量（默认值为 10%）。黄色 (#FFFF00) 表示故障率介于最小阈值和最大阈值之间（10% 和 30%）。红色 (#FF0000) 表示故障率大于最大阈值 (30%)。

增强了自定义字段空值的处理

以下公共 API 请求已更新，以便在自定义字段值为空时返回错误消息：

- 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}

已更新通知端点

以下 REST API 公共端点已更新，以根据用户是否应接收订阅通知返回 notifyUser 字段：

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

新的 BOM 状态端点

已创建一个新的 REST API 端点，以确定何时为给定扫描更新了 BOM：

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

可能的状态值包括 NOT_INCLUDED、BUILDING、SUCCESS、FAILURE。

弃用 PUT /api/settings/auto-remediate-unmapped

在 Black Duck 2022.4.1 中，公共端点 PUT /api/settings/auto-remediate-unmapped 已更改为 PATCH /api/settings/auto-remediate-unmapped，但已弃用 PUT 端点，并保留以保持向后支持性。从该版本开始，PUT /api/settings/auto-remediate-unmapped 端点现在已被删除。

弃用和移除许可证 API 请求

以下 API 请求已被移除：

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

移除 GET api/licenses/{licenseId}/obligations 后，任何 API 将不再返回该义务 API。将改为返回许可条款 API (/api/licenses/{licenseId}/license-terms)。

此外，以下 API 请求已被弃用：

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

新的和增强的组件端点

添加了新的 REST API 端点以获取/修改组件级别上的 SBOM 字段值：

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

以下 REST API 端点已得到增强，可以获取在元数据/链接部分中包括 sbom-field 端点的组件的 SBOM 字段值：

- GET /api/components/{componentId}

新的修补程序 /api/settings/data-retention 端点

新的 PATCH /api/settings/data-retention REST API 端点将替换现有的 PUT /api/settings/data-retention。因此，PUT /api/settings/data-retention 已弃用，并将在即将发布的版本中移除。

新的依赖关系升级指南公共 API 端点

添加了一个新的 REST API 端点，为依赖关系升级指南提供数据：

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

已更新 /api/projects/{projectId}/versions/{projectVersionId}/matched-files 端点

/api/projects/{projectId}/versions/{projectVersionId}/matched-files 端点现在包括一个“matchTypeFilterValue”标志，以便在查看结果时更好地处理不一致问题。下表显示 matchType 如何映射到 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

二进制扫描程序信息

二进制扫描程序已更新为版本：2022.9.1。现在，二进制扫描程序通过软件包管理器支持加入了对 NPM 的支持。

修复了版本 2022.10.0 中的问题

在此发布中修复了客户报告的以下问题：

- (HUB-29825)。修复了以下问题：禁用系统设置“项目经理角色设置 > 安全经理”时，将全局安全经理同时分配给个人和组总体角色会导致不允许进行修复操作（显示为灰色）。
- (HUB-30488)。修复了以下问题：分层 BOM 树间歇性地无法显示子组件（树形结构无法向下展开）。
- (HUB-33274)。更新了 REST API 文档，以包含适用于“BOM 组件展示”的“componentVersionName”和“componentVersion”。
- (HUB-33407)。修复了以下问题：一些用户在代码库大小不受限制时会收到“您已超出可以扫描的最大代码量”通知。
- (HUB-33693)。修复了以下问题：代码段视图中的已上传源窗口可能不会立即显示。
- (HUB-33847)。修复了以下问题：当项目创建请求正文中不存在克隆类别字段 cloneCategories 时，将选择/启用所有克隆类别。此外，通过 API 创建项目时，如果不存在字段 projectLevelAdjustments，则该字段默认为“true”。
- (HUB-33922)。修复了以下问题：“管理”>“诊断”>“作业”中仅显示了 7 天的作业历史记录，而实际应该显示 30 天的作业历史记录。
- （HUB-33945、HUB-34938）。修复了以下问题：在 Black Duck 中为项目生成大型 HTML 漏洞报告导致应用程序崩溃，或花费比预期更长的时间。作为修复的一部分，我们添加了一个可配置的 HUB_MAX_HTML_REPORT_SIZE_KB 属性来管理 HTML 报告下载。此属性仅影响 HTML 报告的查看，而不影响任何其他报告的生成或下载。
- (HUB-33972)。修复了以下问题：使用 OnPrem KB March 数据时，字符串搜索/版权搜索可能无法正常工作。
- (HUB-34085)。修复了以下问题：组件管理页面上的按名称排序区分大小写。
- (HUB-34246)。修复了“项目版本比较”视图相关的浏览器显示问题。
- (HUB-34511)。修复了以下问题：使用中文字符时，依赖关系扫描的项目名称会变成无法读取的字符。
- (HUB-34676)。修复了以下问题：更新禁用的自定义字段会触发所有项目版本的 BOM 计算。
- (HUB-34712)。修复了以下问题：由于 BDBA 容器的运行状况检查超时设置与 Docker Swarm 和 Kubernetes 不同步（30 秒）而导致二进制扫描 Pod 进入 CrashLoopBackOff 状态。此外，现在可以自定义运行状况检查超时，以便进行自定义：
  - 对于 Kubernetes，请使用以下参数，其中 ### 是以秒为单位的值：
    --set binaryscanner.timeout=###
  - 对于 Docker Swarm，请在 docker stack deploy 命令中提供超时值，其中 ### 是以秒为单位的值：

```
BDBA_HEALTH_CHECK_TIMEOUT=### docker stack deploy -c docker-compose.yml -c sizes-
gen03/10sph.yaml -c docker-compose.bdba.yml hub
```

- (HUB-34839)。向 docker-compose.local-overrides.yml 添加了 postgres-upgrader 部分。
- (HUB-34887)。修复了一个气隙环境问题：phone-home 调用可能长时间挂起，导致注册服务无响应时系统行为错误。
- (HUB-35110)。修复了 blackduck-config.env 内针对未映射代码位置的默认保留期的文档。
- (HUB-35140)。修复了以下问题：具有共享漏洞注释的组件的注释不特定于来源。
- (HUB-35184)。已将 Zulu Java 版本升级到 11.0.16+8，以修复 Black Duck 2022.4.2 中发现的漏洞。
- (HUB-35196)。修复了以下问题：使用组件/组件版本过滤器时，未显示组件名称结果。
- (HUB-35222)。修复了以下问题：在浏览特定漏洞 (CVE-2016-1000027) 的页面时，“受影响的项目”选项卡无法加载页面。
- (HUB-35366)。修复了以下问题：“组件详细信息”屏幕中未显示自定义字段值。
- (HUB-35369)。修复了以下问题：打印 Black Duck BOM pdf 时，报告在页面边缘重叠，无法正确列出所有组件。
- (HUB-35407)。修复了以下问题：具有空值的自定义字段会导致 KbUpdateWorkflowJob-Component 版本更新作业失败。
- (HUB-35524)。修复了使用 /api/projects/<project_id>/versions/<version_id>/policy-rules 公共端点时的用户权限问题。
- (HUB-35660)。修复了扫描客户端中的重复条目 ID 问题，该问题可能导致退出代码 70 – “java.util.ConcurrentModificationException”错误。

Black Duck SCA 2022.7.x

版本 2022.7.2 的公告

目前尚未发布有关 Black Duck 2022.7.2 的新公告。

版本 2022.7.2 中的新增功能和更改功能

Black Duck 2022.7.2 中没有新增或更改的功能。

容器版本

- 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 增强

Black Duck 2022.7.2 中没有新增或更改的 API 请求。有关 API 请求的更多信息，请参阅 Black Duck 中提供的《REST API 开发人员指南》。

修复了版本 2022.7.2 中的问题

在此发布中修复了客户报告的以下问题：

- (HUB-35687)。修复了以下问题：当 CVE 和 BDSA 漏洞相关时，相关漏洞会错误地添加到漏洞修复中。如果发生这种情况，当应用到存在此问题的组件时，vulnerable-bom-components API 将返回“HTTP 响应 400/错误请求”错误。

版本 2022.7.1 的公告

目前尚未发布有关 Black Duck 2022.7.1 的新公告。

版本 2022.7.1 中的新增功能和更改功能

Git 存储库 SCM 集成 - 阶段 2

Black Duck 2022.7.1 更新了用户在创建项目和版本时添加存储库/分支字段的方式。现在，您可以添加授权的 SCM 提供商（目前仅限 GitHub Standard 和 GitHub Enterprise），然后在创建新项目时可以选择这些提供商。这样做之后，将自动在新项目的“项目设置”页面中预填充存储库 URL 和分支版本。

此功能与 Detect 8.x 及更高版本兼容，并将在新的扫描中生效。

请注意，在 Black Duck 中默认情况下不启用 SCM 集成，必须通过在您的环境中添加以下内容来激活此功能：

对于 Swarm 用户，请将以下内容添加到您的 blackduck-config.env 文件中：

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

对于 Kubernetes 用户，请将以下内容添加到您的 values.yaml 文件中的 environs 部分下：

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

新热图数据下载

您现在可以下载热图数据，该热图数据保存系统中的终端扫描信息。您可以转至管理 > 诊断 > 系统信息下载此信息。从此处单击下载热图 (.zip) 按钮。输出为 .csv 文件。

结合使用 UTF8 与 BOM 创建报告

请注意，Black Duck 2022.7.0 中添加了此功能，但在该版本的发行说明中意外忽略了此功能。

Black Duck 2022.7.0 引入了对 UTF8 BOM 字符编码的支持，可在使用非西方字符的客户的报告中使用此编码。要启用此功能，请将以下内容添加到 blackduck-config.env 文件中：

```
USE_CSV_BOM=true
```

项目版本组件的新批量操作

批量更新功能现在支持对项目版本页面上的组件执行以下操作：

- 忽略/取消忽略组件
- 设置组件用法类型
- 设置通知文件中的包含/排除

容器版本

- 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 增强

有关新增或更改的 API 请求的详细信息，请参阅 Black Duck 中提供的 API 文档。

新的扫描监控 API 端点

添加了一个新的 REST API 端点，它可分析扫描错误率，并允许您在给定的时间范围内（默认设置为上一小时）从系统中的终端扫描获取扫描监控信息：

- GET /api/scan-monitor

请求参数如下：

- level （必填）。数值 1 或 2 或 3，默认值为 “1” 。
  请求示例： GET /api/scan-monitor?level=1

  级别 1 是简单的二进制响应，要么为 OK，要么为 NOT OK（如果故障率超过设置的最大阈值 [默认值为 30%]）。

级别 2 返回十六进制颜色代码（绿色、黄色或红色），具体取决于状态。绿色 (#00FF00) 表示在监控的时间范围内（默认值为上一小时）的故障率小于设定的最小阈值量（默认值为 10%）。黄色 (#FFFF00) 表示故障率介于最小阈值和最大阈值之间（10% 和 30%）。红色 (#FF0000) 表示故障率大于最大阈值 (30%)。

级别 3 根据扫描状态返回汇总的扫描计数。

可在 blackduck-config.env 文件中，为环境配置监控时间范围、最小和最大阈值。

增强了自定义字段空值的处理

以下公共 API 请求已更新，以便在自定义字段值为空时返回错误消息：

- 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}

修复了版本 2022.7.1 中的问题

在此发布中修复了客户报告的以下问题：

- (HUB-33693)。修复了以下问题：除非点击面板，否则不会加载包含代码段的文件的扫描文件视图。
- (HUB-34246)。修复了打印“项目版本比较”视图时的浏览器显示问题。
- （HUB-34472、HUB-34781、HUB-34682）。修复了一个问题：在“组件版本”页面上移除许可证后，此操作不会反映在 BOM 报告中。
- (HUB-34511)。修复了以下问题：从 HTTP 标头而不是 BDIO 标头提取项目和版本名称，从而导致在使用非拉丁字符时字符不可读。
- (HUB-34618)。提高了生成有关 KB 本地环境的“版本详细信息”报告时的性能。
- (HUB-35110)。修复了 blackduck-config.env 内针对未映射代码位置的默认保留期的文档。
- (HUB-35196)。修复了以下问题：使用组件/组件版本过滤器时，未显示组件名称结果。
- (HUB-35222)。修复了以下问题：在浏览特定漏洞 (CVE-2016-1000027) 的页面时，“受影响的项目”选项卡无法加载页面。
- (HUB-35304)。修复了以下问题：升级到 2022.7.0 时，分配给用户组的超级用户角色未迁移到 2022.7.0 中引入的新角色。
- (HUB-35349)。修复了以下问题：由于匹配过程完成后发送消息，快速扫描在升级到 Black Duck 2022.7.0 后可能失败。当环境中运行多个匹配容器时，更有可能发生这种情况。
- (HUB-35407)。修复了以下问题：具有空值的自定义字段会导致 KbUpdateWorkflowJob-Component 版本更新作业失败。

版本 2022.7.0 的公告

弃用 PostgreSQL 9.6

正如之前宣布的，对于在 PostgreSQL 9.6 上运行 Black Duck 的支持已在 2021.6.0 版本的 Black Duck 结束。从 2022.7.0 版本的 Black Duck 开始，尝试使用 PostgreSQL 9.6 运行 Black Duck 将会生成错误，且 Black Duck 将无法启动。

即将弃用 PostgreSQL 11

对在 PostgreSQL 11 上运行 Black Duck 的支持将在 2022.10.0 版本结束。从该版本开始，尝试使用 PostgreSQL 11 运行 Black Duck 将会生成错误，且 Black Duck 将无法启动。

PostgreSQL 容器从版本 11 迁移到版本 13

Black Duck 在 2022.10.0 版本中，将其 PostgreSQL 映像从版本 11 迁移到版本 13。不使用 Black Duck 提供的 PostgreSQL 映像的客户不会受到影响。

即将进行的自定义字段 API 更改

在 2023.1.0 版本的 Black Duck 中，以下 API 将更改为在尝试读取或更改已禁用的自定义字段时返回错误。需要重新启用该字段，才能访问它。

- `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}`

不再支持旧版特征扫描和旧版软件包管理器扫描

此功能将在 Black Duck 2023.7.0 版本中正式弃用。

客户应升级到 Detect 8.x 以确保兼容性。Detect 8.x 暂定于 2022 年 5 月/6 月发布，与 Black Duck 2022.7.0 版本以及此弃用发行说明一致。这将为客户提供一年的 Detect 升级周期，以便与未来的弃用日期保持一致。

Helm2 支持即将结束

从 2023.1.0 版本开始，Black Duck 将不再支持针对 Kubernetes 部署的 Helm2。Kubernetes 的最低支持版本将增加到 1.13（Helm3 支持的最旧版本）。

更正：Git 存储库 SCM 集成 - 阶段 1

2022.4.0 发行说明中提供的、有关为 Swarm 用户启用 Black Duck 中的 Git 存储库 SCM 集成的说明不正确。正确的变量设置如下：

对于您的 docker-compose.yaml webapp 环境：

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

此外，在 blackduck-config.env 文件中添加以下内容：

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

已更新 PostgreSQL 支持时间表

从即将发布的 2022.10.0 版本开始，Black Duck 将终止对外部 PostgreSQL 11 的支持。请参阅下表，了解对未来 PostgreSQL 版本支持的开始和结束日期。

PG 版本	首次发布	最新发布	BD 外部支持添加	BD 外部支持结束
16.x	2023 年末	2028 年末	2024.7.0	2026.10.0
15.x	2022 年末	2027 年末	2023.7.0	2025.10.0
14.x	2021 年 9 月	2026 年 11 月	2022.7.0	2024.10.0
13.x	2020 年 9 月	2025 年 11 月	2021.8.0	2023.10.0
12.x	2019 年 10 月	2024 年 11 月	X	X
11.x	2018 年 10 月	2023 年 11 月	2020.6.0	2022.10.0

日语

2022.4.0 版本的 UI、联机帮助和发行说明已本地化为日语。

简体中文

2022.4.0 版本的 UI、联机帮助和发行说明已本地化为简体中文。

版本 2022.7.0 中的新增功能和更改功能

对外部数据库的 PostgreSQL 14 支持

Black Duck 对于使用外部 PostgreSQL 的新安装，现在支持并建议使用 PostgreSQL 14。迁移到 Black Duck 2022.7.x 不需要迁移到 PostgreSQL 14。

内部 PostgreSQL 容器的用户无需执行任何操作。

注：由于 PostgreSQL 14.0 到 14.3 中的索引损坏错误，支持的最低 PostgreSQL 14 版本是 14.4。

将超级用户角色拆分为管理员域角色

目前，任何具有“超级用户”角色的 Black Duck 用户都可以创建/修改所有用户的权限，以便他们可以将系统管理员角色分配给任何用户，包括他们自己的用户。这将导致任何超级用户能够完全访问和控制 Black Duck 实例，包括 SysAdmin 角色。这似乎是一个权限升级缺陷，但角色可按预期正常工作。

为了防止出现这种情况，移除了“超级用户”角色并创建了新角色，以处理以前与它关联的各种职责：“全局项目管理员”、“全局项目组管理员”、“用户管理员”和“自定义字段管理员”。有关这些新角色的更多信息，请参阅 Black Duck 帮助。

新基础设施即代码 (IaC) 问题显示

应用程序不仅仅是应用程序代码，基础设施和部署方法是确保应用程序安全性的关键组件。因此，IAC 被用于在不同的云和本地环境中实现应用程序部署和设置的自动化。这些配置选项在确保应用程序安全性方面发挥着关键作用，对于容器化或基于服务的应用程序尤其重要。

现在，在 Black Duck 2022.7.0 中，如果扫描包含 IaC，则在查看项目版本页面的 BOM 时，您可以看到 IaC 问题。显示的信息将为您提供对代码中发现的任何潜在问题采取行动所需的信息。

请注意，要运行 IaC 扫描，您必须满足以下操作系统要求，并具有 Detect 7.14 或更高版本。

有关“基础设施即代码”扫描的详细信息，请参阅我们的社区页面。

改进了扫描 CLI 的稳定性

通过引入重试机制，改进了扫描 CLI，以防止在服务器上完成时挂起。这意味着即使在 Hub、扫描或 nginx 服务重新启动后，扫描仍将完成并正常上传。

新增了对项目版本组件批量注释的支持

此新功能提供了添加批量注释的功能，以方便用户审阅和策划 BOM。例如，您可以在项目版本页面上选择任意数量的组件，并同时向所选项目添加注释，而不是单独对组件应用注释。

新的自动化 API 访问令牌清除

这一新功能将使 Black Duck 系统的用户管理员能够通过访问令牌更好地维护和控制对 Black Duck 的访问，方法是设置自动清除非活动访问令牌的计划。此功能可在新的管理员 > 访问令牌页面中找到。您也可以通过此页面手动策划所有现有访问令牌。

增加了二进制扫描容器内存分配

为了防止二进制扫描失败，我们将二进制扫描容器内存从 2GB 增加到了 4GB。

增强了策略规则用户体验

创建或编辑策略时，组件条件现在将显示说明，以阐明在使用“在内部”或“不在内部”运算符时如何向策略添加或排除组件版本。

更新了 Black Duck KnowledgeBase 搜索

查找 > Black Duck KnowledgeBase 页面对其外观以及执行搜索后显示结果的方式进行了一些细微更改。

在早期版本中，Black Duck KnowledgeBase 搜索在结果集内显示 Black Duck 项目和自定义组件以及 KnowledgeBase 组件。从 2022.7.0 开始，Black Duck KnowledgeBase 搜索仅返回 KnowledgeBase 组件数据。为了搜索自定义组件，用户应利用“组件”搜索选项卡。要搜索 Black Duck 项目，用户应使用“项目”搜索选项卡。

此外，Black Duck KnowledgeBase 页面上的“组件来源”过滤器（自定义组件和 Black Duck 项目）已被移除。

增强了知识库更新作业任务

以前，组成知识库更新作业的任务（组件、组件版本、许可证、NVD 漏洞和 BDSA 漏洞）按预设顺序运行。如果组件任务失败，则不会执行后续任务。作为 2022.7.0 的新功能，引入了一种管理失败任务的继续机制，防止阻止后续任务的执行。

此外，从作业页面的角度来看，这提供了更好的视觉效果，前提是存在一些关于特定任务失败原因的细节。

已添加新的快速扫描属性

以下属性已添加至快速扫描的输出：

- cweIds：此安全漏洞的常见弱点枚举 (CWE) ID 列表。
- shortTermUpgradeGuidance：建议升级到的组件版本（作为解决此漏洞的短期行动），因为它与使用中的主要版本相同。
- longTermUpgradeGuidance：建议升级到的组件版本（作为长期行动）。采取此行动可能需要升级主要版本号，并且必须更仔细地进行规划。

为 Detect 端点新增的升级指导信息

以下内容已添加到 Detect 组件扫描结果中：

- shortTermUpgradeGuidance：建议升级到的组件版本（作为解决此漏洞的短期行动），因为它与使用中的主要版本相同。
- longTermUpgradeGuidance：建议升级到的组件版本（作为长期行动）。采取此行动可能需要升级主要版本号，并且必须更仔细地进行规划。

更新了项目版本的数据保留管理

现在，您可以更好地管理项目版本的数据保留策略。如果在您的环境中启用了自动数据移除，您现在可以选择特定的项目版本以防止删除。这可以在创建新项目或编辑现有项目版本时启用。查看项目时，不受自动数据移除影响的项目版本将在其行末尾显示一个锁定图标。

更新的软件材料清单 (SBOM) 报告类型和导出格式

您现在可以用 CycloneDX v1.4 格式导出项目的软件材料清单报告。CycloneDX v1.4 格式包含安全漏洞信息；BDSA 记录现在将与 NVD 记录一起包含在内。

有关 CycloneDX v1.4 的更多信息，请访问 CycloneDX v1.4 参考页面。

报告类型（SPDX、Cyclonev DX 1.3 或 CycloneDX v1.4）也将包含在报告名称中，以便生成报告后更好地识别使用的类型。

此外，生成 SBOM 报告时还提供了新的报告格式。您现在可以从 JSON、YAML、RDF 和 tag:value 中进行选择，以作为报告的输出。

新的数据库分区作业

日志表现在按月进行分区。第一个分区是特殊的，它包含所有现有的日志事件。JournalPartitionMaintenanceJob 作业为项目审核跟踪创建新的数据库分区，并删除早于 5 年的旧分区和日志事件。

扫描状态/状态重构

以前，扫描状态是扫描状态和扫描进度的设计组合，在当前基于队列的扫描架构中无法正常工作。新方法将提供一种状态，然后提供一种方法用于跟踪扫描在系统中的进度。此方法足够灵活，以便可以对传统扫描架构进行改造，因此使用了单一方法。状态应该保留在数据库中，而进度由于是瞬态的，更新比较频繁，因此应该移到缓存中。

报告数据库增强

已在 reporting.component_vulnerability 具体化视图中添加 exposed_on 字段。

轻微的报告模式更改

在 2023.1.0 中，reporting.scan_view 中 basedir 列的类型将从 character varying 更改为 text，以容纳长度超过 255 个字符的路径。

支持的浏览器版本

- Safari 版本 15.5 (17613.2.7.1.8)
  - 不再支持 Safari 13.0 和更低版本
- Chrome 版本 103.0.5060.114（正式版本）(x86_64)
  - 不再支持 Chrome 版本 71 和更低版本

- Firefox 版本 102.0（64 位）
  - 不再支持 Firefox 版本 71 和更低版本
- Microsoft Edge 版本 103.0.1264.44（正式版本）（64 位）
  - 不再支持 Microsoft Edge 版本 78 和更低版本

容器版本

- 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 增强

有关新增或更改的 API 请求的详细信息，请参阅 Black Duck 中提供的 API 文档。

用于下载 Sigma Scanner 的新 API

已创建一个新端点，可直接从 upload-cache 下载 Sigma 二进制文件。API 请求有一个路径变量 arch（需要该变量来指示所需架构），以及一个名为 version 的可选标头参数。

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

修复了版本 2022.7.0 中的问题

在此发布中修复了客户报告的以下问题：

- (HUB-33231)。已修复一个问题，其中，“扫描”页面上按扫描尺寸对扫描进行排序时，未按正确顺序显示列表。
- (HUB-33974)。修复了漏洞的受影响项目计数可能产生误导的问题。忽略组件将会更改摘要页面上具有给定风险的组件数量。漏洞搜索不会统计被忽略的组件，但组件搜索会。

- (HUB-32773)。修复了以下问题：在本地修改组件时，会导致我们的系统将其视为本地组件，而不是源自 KnowledgeBase 的组件。获取组件的新信息时，BOM 计算不会查询 KnowledgeBase。
- (HUB-34468)。修复了以下问题：快速扫描在队列中等待其他运行时间较长的扫描类型完成匹配时会超时。
- (HUB-34459)。修复了与传统 scan.cli 一起使用时 --matchConfidenceThreshold 参数无法正常工作的问题。
- (HUB-33477)。修复了以下问题：禁用 SAML 时 Black Duck 元数据 URL 下载按钮可用。
- (HUB-33549)。修复了以下问题：“策略管理 > 创建策略规则 > 组件条件”的“匹配类型”选择列表没有“直接依赖关系二进制”和“传递依赖关系二进制”选项。
- (HUB-34215)。更新了 jackson-databind 和 gson 组件，以响应发现 4 个高风险漏洞。
- (HUB-33551)。修复了上传带有空代码位置的 BDIO 文件失败且状态代码为 400 的问题。
- (HUB-32919)。修复了以下问题：尝试使用聚合模式 BDIO 从 Hub 下载扫描时会生成 0 字节的损坏/空 BDIO。
- (HUB-29445)。修复了项目 REST API 过滤不支持包含逗号的项目名称的问题。
- (HUB-33164)。修复了当系统日志过大时无法从 Blackduck UI 下载的问题。
- (HUB-34282)。修复了 system_check.sh 脚本的一个问题：如果内存限制和预留设置为超过 Java 堆大小 512MB，则可能会产生错误警告。脚本已更新为在开销的内存大于 20% 且大于 1024Mb 时进行标记，以便根据文档进行设置时，更小的容器不会导致错误警告。
- (HUB-33923)。修复了以下问题：刷新管理 > 诊断 > 系统信息 > 作业页面时，作业历史记录的统计信息会显示明显不同的计数。
- (HUB-34195)。更新了 REST API 文档，以从“创建版本报告”一节（或 /api/versions/{projectVersionId}/reports 请求）中移除 SBOM（作为 reportType 的值）。
- (HUB-34296)。修复了以下问题：由于 i18n 字符不正确而无法在日语设置中显示策略覆盖日期信息。
- (HUB-32008)。修复了以下问题：由于 QuartzVersionBomEventCleanupJob 作业未自动清理“最新但有错误”事件，导致“安全风险排名”页面停留在“处理中”状态。
- (HUB-33727)。修复了更新漏洞的修复状态或注释时的 UI 错误（在“项目版本”的“安全性”选项卡中）。
- (HUB-33691)。修复了一个 UI 错误：具有已知弱点的加密算法的“加密”选项卡上缺少警告图标。
- (HUB-34240)。修复了 /api/projects/{projectId}/custom-fields/{customFieldId} 请求存在的问题：在发布空值时，请求可能生成 400 错误。
- (HUB-34246)。修复了“项目版本比较”视图上的浏览器显示问题。
- (HUB-33246)。阐明了 REST API 文档；为 https://<server-url>/api/ 替换了对 https://.../ 的引用。
- (HUB-33481)。修复了 2021.8.x 和更高版本之间的 /api/projects/{pid}/versions/{vid}/matched-files?offset={larger than totalCount} 响应不一致的问题。matched-files 端点现在应始终返回一个 200 OK 响应，其中包含空项目，即使 offset > totalCount 也是如此。
- (HUB-34468)。修复了以下问题：快速扫描失败并显示以下错误：“获取开发人员扫描结果时出错。可能已发生超时。”或由于匹配引擎中的延迟而导致的“HTTP 404 未找到”响应。
- (HUB-33512)。更新了管理 > 设置 > 用户验证下的“测试连接”、“用户身份验证”和“字段映射”的文本。移除了“并显示映射测试用户元数据的结果”的提法。
- (HUB-34836)。修复了以下问题：启用 BLACKDUCK_HUB_SHOW_UNMATCHED 标志时，可以像编辑项目本身一样编辑未匹配的组件。

- (HUB-34380)。修复了以下问题：尝试将新版本扫描到已进行大量调整的项目时，会导致新版本的 BOM 扫描在服务器上失败，并显示消息“太多参数发生异常”。
- (HUB-33793)。修复了以下问题：在使用未以“Black Duck Security Advisory”授权的注册密钥并更改安全风险等级时，“项目版本”详细信息报告会失败。
- (HUB-33375)。修复了查询构建代码中的一些错误 SQL 语法，其中，ORDER_BY 在确定排序依据字段的循环之外。如果没有排序字段，ORDER_BY 将为空。
- (HUB-34780)。修复了以下问题：即使创建或删除了超过 500 个项目/版本，“管理”>“诊断”>“使用：项目”>“Project_created/Version_Created/Version_Deleted”的统计信息仍限制为 500。
- (HUB-34592)。修复了没有匹配的组件、但空组件和现有组件都在测试中失败时的 CodeLocationBomMatchCacheEntry 反序列化错误。
- (HUB-34588)。修复了以下问题：由于链接中的哈希字符未编码，导致 conan 包的版权链接无法正常工作。
- (HUB-24664)。修复了以下问题：BDSBackgroundUpdateWorker 仍尝试通过 HTTP 而不是 HTTPS 与注册服务器通信。
- (HUB-33679)。修复了以下问题：启用 MaaS 的扫描在提取复合元素时有时会失败。
- (HUB-34218)。更新了 REST API 文档，以包含适用于“BOM 组件展示”的“componentVersionName”和“componentVersion”。

Black Duck SCA 2022.4.x

版本 2022.4.2 中的新增功能和更改功能

提高了数据库迁移脚本的性能

升级 Black Duck 版本时使用的数据库迁移脚本的性能得到了改进，从而缩短了安装时间。

容器版本

- 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 增强

有关新增或更改的 API 请求的详细信息，请参阅 Black Duck 中提供的 API 文档。

修复了版本 2022.4.2 中的问题

Black Duck 2022.4.2 不包含客户报告的已修复问题。

版本 2022.4.1 中的新增功能和更改功能

新的 BDSA 自动修复设置，用于自动忽略具有相关的不匹配 BDSA 记录的 CVE

激活此设置会将修复状态设置为 IGNORED 并添加一条消息来说明修复漏洞的原因，从而自动修复具有相关未映射 BSSA 的新 CVE 漏洞。

此新设置仅适用于具有相关 BDSA 漏洞的 CVE 漏洞。如果 CVE 映射到组件版本，但其相关 BDSA 还未映射到该组件版本，则系统可能会根据系统设置自动修复 CVE 漏洞。

可以在“管理员”>“系统设置”>“BDSA 自动修复”页面上启用 BDSA 自动修复功能。

已添加新的快速扫描属性

以下属性已添加至快速扫描的输出：

- cweIds：此安全漏洞的常见弱点枚举 (CWE) ID 列表。
- shortTermUpgradeGuidance：建议升级到的组件版本（作为解决此漏洞的短期行动），因为它与使用中的主要版本相同。
- longTermUpgradeGuidance：建议升级到的组件版本（作为长期行动）。采取此行动可能需要升级主要版本号，并且必须更仔细地进行规划。

改进了用户权限评估性能

对大多数 API 请求的用户权限评估进行了改进。这将导致更一致的加载时间（包括加载 BOM），而不考虑用户的角色或权限。

更新了 Black Duckctl

Black Duckctl 已更新到 3.0.1，以添加适用于 sizes-gen03 部署大小的 Black Duck 2022.4 0 安装支持。

容器版本

- 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 增强

有关新增或更改的 API 请求的详细信息，请参阅 Black Duck 中提供的 API 文档。

项目端点的性能改进

发现以下 API 项目端点性能不佳并已进行优化：

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

修复了版本 2022.4.1 中的问题

在此发布中修复了客户报告的以下问题：

- （HUB-32395、HUB-33033）。修复了以下问题：SPDX 报告中有时不显示匹配组件修改后的已声明许可证。
- (HUB-29532)。已修复一个问题，其中，当发行版映像中的 rootfs 路径不是从根目录开始，而是从子目录开始时，Linux 发行版软件包匹配中断。
- (HUB-33947)。修复了从“受影响的项目”页面更新修复状态时未更新安全风险的问题。
- (HUB-33551)。修复了以下问题：上传代码位置名称为空的 BDIO 文件时，请求会失败，返回状态代码 400 并在后台引发异常。
- (HUB-34065)。修复了 SPDX 验证工具中导致以下错误的 SPDX 2.2 报告格式：
  `########[################## {"pointer":"/packages/0"} # ["packageSupplier"]`
- (HUB-33616)。修复了以下问题：在某些情况下（当扫描的存档中有重复的存档条目时），扫描客户端生成 ID 不正确的 BDIO，因而在将 BDIO 文件存储到数据库时会产生错误。
- （HUB-33915、HUB-33865）。修复了以下问题：扫描上传 API 将整个扫描数据作为一条消息提交到 RabbitMQ 而不进行分块，从而导致出现消息大小错误。
- (HUB-24664)。修复了注册容器日志显示尝试通过 HTTP 进行通信的问题。
- (HUB-33579)。修复了与传统 scan.cli 一起使用时 --matchConfidenceThreshold 参数无法正常工作的问题。
- (HUB-33311)。修复了特征扫描程序可能失败并显示错误代码 74 的问题。引入了重试功能以缓解此错误。

版本 2022.4.0 的公告

Spring 框架的安全公告 (CVE-2022-22965)

Black Duck 已注意到与 Spring 框架开源软件相关的已披露的安全问题 CVE-2022-22965（在 Black Duck KnowledgeBase™ 中跟踪为 BDSA-2022-0858）（于 2022 年 3 月 30 日披露）。有关此漏洞的详细信息，请参阅官方的 CVE 条目：https://tanzu.vmware.com/security/cve-2022-22965

2022 年 3 月 31 日，Spring 发布了 Spring 框架版本 5.3.18 和 5.2.20，这些版本解决了 CVE-2022-22965 描述的漏洞。

目前，Black Duck 认为 Black Duck SIG 产品、服务和系统面临的风险有限。在我们已经接触到的风险范畴内，我们已采取了一些缓解措施，以防止有人试图利用漏洞。我们已完成所有内部调查，这些调查的结果可在我们的社区通告页面的“产品状态”部分中找到。

最后，在此说明，前面提到的调查只关注 CVE-2022-22965（Spring 框架），不应与 CVE-2022-22963（Spring Cloud 功能）混淆。

在发布时，Black Duck 尚未识别出 SIG 产品中面临的任何 CVE-2022-22963（在 Black Duck Hub KnowledgeBase™ 中跟踪为 BDSA-2022-0850）风险。如果有改变此评估的新详细信息可用，将发布有关 CVE-2022-22963 的单独通告。

升级到 Black Duck 2022.4.0

请注意，由于执行迁移脚本和此版本中引入的其他新流程，升级到 Black Duck 2022.4.0 所需的时间可能比预期的长。更多详细信息可在下面的“新增功能和更改功能”部分中找到。

资源指导变更

默认资源设置已更新，所有扫描卷的建议设置均已增加。以前的资源设置仍然可用，并已按如下所述移至新目录，但不建议使用这些设置。

请注意，确切的扫描吞吐量可能会因扫描大小、类型和成分而异。但是，我们在内部测试中使用了此细分来收集下表中的信息：

- 50% 完整特征扫描
- 40% 完整软件包管理器扫描
- 10% 开发者软件包管理器扫描

容器资源限制

从 Black Duck 2022.4.0 开始，所有容器都将设置资源限制，而以前，有些容器没有设置资源限制。例如，以前的资源分配没有为 bomengine 容器设置 CPU 限制，因此它使用的 CPU 可能与具有限制的容器不相称。由于以下新的大小不允许使用无限的 CPU，因此，如果客户选择接近旧限制的新大小，扫描吞吐量可能会下降。

文件组织更改

除上述更改外，资源覆盖 YAML 文件的组织也发生了变化。

对于 Kubernetes，Helm 图表中的资源覆盖 YAML 文件的组织发生了变化：

- values 文件夹已重命名为 sizes-gen01。
- 之前的 4 个 T 恤尺寸文件（small.yaml 等）已被移至新的 sizes-gen02 目录中。
- 新目录 sizes-gen03 现在包含下表中命名的每个配置的资源覆盖文件；这些文件被命名为 10sph.yaml、120sph.yaml 等。

对于 Swarm，Black Duck 将不再直接在 docker-compose.yml 中分配容器资源。将改为在单独的覆盖文件中指定资源。以前的资源分配（来自 Black Duck 版本 2022.2.0 和更早版本）已移至 sizes-gen02/resources.yaml。从 Black Duck 2022.4.0 及更高版本开始，将在 sizes-gen03 folder 中提供多个可能的分配。

对于 Kubernetes 和 Swarm，将根据测得的负载即每小时平均扫描数进行 7 次分配；如果您的预期负载与其中一个预定义的分配不匹配，请对其进行取整。例如，如果预计每小时扫描 100 次，请选择 sizes-gen03/120sph.yaml。

资源指导和容器可扩展性

这些设置应用于 Kubernetes 和 Swarm 安装。

名称	扫描次数/小时	Black Duck 服务	PostgreSQL	总数
10sph	10	CPU：12 核 内存：30 GB	CPU：2 核 内存：8 GB	CPU：14 核 内存：38 GB
120sph	120	CPU：13 核 内存：46 GB	CPU：4 核 内存：16 GB	CPU：17 核 内存：62 GB
250sph	250	CPU：17 核 内存：118 GB	CPU：6 核 内存：24 GB	CPU：23 核 内存：142 GB
500sph	500	CPU：28 核 内存：210 GB	CPU：10 核 内存：40 GB	CPU：38 核 内存：250 GB
1000sph	1000	CPU：47 核 内存：411 GB	CPU：18 核 内存：72 GB	CPU：65 核 内存：483 GB
1500sph	1500	CPU：66 核 内存：597 GB	CPU：26 核 内存：104 GB	CPU：92 核 内存：701 GB
2000sph	2000	CPU：66 核 内存：597 GB	CPU：34 核 内存：136 GB	CPU：100 核 内存：733 GB

PostgreSQL 设置

使用 PostgreSQL 容器的客户需要使用 ALTER SYSTEM 手动设置值，而对 shared_buffers 的更改将在下一次重新启动 PostgreSQL 后才会生效。这些设置应用于 Kubernetes 和 Swarm 安装。

名称	扫描次数/小时	PostgreSQL CPU/内存	shared_buffers (MB)	effective_cache_size (MB)
10sph	10	CPU：2 核 内存：8 GB	2654	3185
120sph	120	CPU：4 核 内存：16 GB	5338	6406
250sph	250	CPU：6 核 内存：24 GB	8018	9622
500sph	500	CPU：10 核 内存：40 GB	13377	16053
1000sph	1000	CPU：18 核 内存：72 GB	24129	28955
1500sph	1500	CPU：26 核	34880	41857

		内存：104 GB		
2000sph	2000	CPU：34 核 内存：136 GB	45600	54720

即将弃用 PostgreSQL 9.6

正如之前宣布的，对于在 PostgreSQL 9.6 上运行 Black Duck 的支持已在 2021.6.0 版本的 Black Duck 结束。从 2022.7.0 版本的 Black Duck 开始，尝试使用 PostgreSQL 9.6 运行 Black Duck 将会生成错误，且 Black Duck 将无法启动。

RHEL 7 和 CentOS 7 上对 Desktop Scanner 的支持终止

从 2022.4.0 开始，Black Duck 将不再为 Red Hat Enterprise Linux 7 和 CentOS 7 构建新版本的 Desktop Scanner。此外，在即将发布的 2022.7.0 版本中，将完全删除这些二进制文件。

已更新 PostgreSQL 支持时间表

从即将发布的 2022.10.0 版本开始，Black Duck 将终止对外部 PostgreSQL 11 的支持。请参阅下表，了解对未来 PostgreSQL 版本支持的开始和结束日期。

PG 版本	首次发布	最新发布	BD 外部支持添加	BD 外部支持结束
16.x	2023 年末	2028 年末	2024.7.0	2026.10.0
15.x	2022 年末	2027 年末	2023.7.0	2025.10.0
14.x	2021 年 9 月	2026 年 11 月	2022.7.0	2024.10.0
13.x	2020 年 9 月	2025 年 11 月	2021.8.0	2023.10.0
12.x	2019 年 10 月	2024 年 11 月	X	X
11.x	2018 年 10 月	2023 年 11 月	2020.6.0	2022.10.0

Azure PostgreSQL 13 Flex Server 配置

安装 Black Duck 时，Azure 用户在运行 external-postgres-init.pgsql init 脚本时可能会遇到以下错误消息：

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

为防止出现此错误，请确保使用 Azure PG 13 Flex Server 时服务器参数“azure.extensions”具有值“PGCRYPTO”。

已弃用的 API

以下传统 API Solr 端点已被弃用，将在 Black Duck 2022.7.0 版本中移除：

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

日语

2022.2.0 版本的 UI、联机帮助和发行说明已本地化为日语。

简体中文

2022.2.0 版本的 UI、联机帮助和发行说明已本地化为简体中文。

版本 2022.4.0 中的新增功能和更改功能

Spring 框架更新

Spring 框架已更新至 5.3.18，以解决严重的 CVE-2022-22965 漏洞。

新的漏洞指标比较

此新功能对漏洞的“概述”页面进行了更改，以便您现在可以在适用的情况下查看指标的并排视图。查看同时具有 BDSA 和 NVD 记录的漏洞时，您将在“得分和指标”部分看到一个图表，比较两种漏洞类型：BDSA 和 NVD。您还可以在 CVSS v2 和 CVSS v3.x 之间进行切换以获取更多信息。

Git 存储库 SCM 集成 - 阶段 1

Black Duck 2022.4.0 将引入一种方法，通过利用集成来管理存储库、分支、构建和版本，从而简化客户新项目的纳管过程。从阶段 1 开始，我们将向“创建项目模式和项目设置”页面添加新的 SCM URL 字段，并向“项目版本设置”页面添加“SCM 分支”字段。

这些字段在此阶段手动填充。但是，在即将发布的 Detect 版本中，它们将在扫描 git 存储库后自动填充。Detect 将自动识别关联的 git 存储库 URL 和分支，然后将该信息发送给 Black Duck。

请注意，在 Black Duck 中默认情况下不启用此功能，必须通过在您的环境中添加以下内容来激活此功能：

对于 Swarm 用户，请将以下内容添加到您的 docker-compose.yml webapp 环境：

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

对于 Kubernetes 用户，请将以下内容添加到您的 webapp 容器环境：

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

BDSA 漏洞的全新“组件”选项卡

BDSA 漏洞记录中添加了一个新的“组件”选项卡。此选项卡将允许您查看受特定 BDSA 漏洞影响的所有已知组件版本。

增强的组件仪表板具体化视图查询

与 SearchDashboardRefreshJob 相关的所有查询都已优化，以获得更好的性能。LicenseDashboardRefreshJob 的可用时间更长，与之相关的视图将在 SearchDashboardRefreshJob 下刷新。这意味着“许可证管理”页面中显示的计数现在将在 SearchDashboardRefreshJob 完成时更新。

注意：由于这些更改，执行迁移脚本会导致升级到 Black Duck 2022.4.0 的过程可能需要比平常更久的时间。

PostgreSQL 11 容器迁移

在使用 Black Duck 提供的 PostgreSQL 容器的 Kubernetes 和 OpenShift 部署中，不再需要 2022.2.0 中添加的以下持久性卷声明。可以安全地删除它及其关联的持久性卷。

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

已更新 Java 堆大小分配和新的环境变量

在以前的版本中，允许 Java 缓慢地将堆大小增加到最大 HUB_MAX_MEMORY。从 Black Duck 2022.4.0 开始，为了充分利用效率和可预测性，我们现在将在启动时预先分配整个 HUB_MAX_MEMORY。

作为此更新的一部分，添加了一个新的环境变量：HUB_MIN_MEMORY。此变量允许您设置 Java 堆大小的下边界。

默认情况下，作为最佳设置，HUB_MIN_MEMORY 设置为等于 HUB_MAX_MEMORY，但可以明确设置为更小的值（例如 512m），以再次允许 Java 从 HUB_MIN_MEMORY 起逐渐获取内存，最大不超过 HUB_MAX_MEMORY。

将快速扫描策略覆盖限制为特定漏洞

在以前的 Black Duck 版本中，策略和组件可能会覆盖快速扫描策略违规。但是，如果随后发现新的漏洞，现有的覆盖可能会抑制违规，从而导致漏报。

现在，在 Black Duck 2022.4.0 中，您现在可以使用现有的 YAML 上传机制在快速扫描中覆盖特定漏洞。

验证漏洞 ID 以匹配预期格式。

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

已添加新的快速扫描漏洞属性

以下属性已添加至快速扫描输出中的漏洞：

- publishedDate（日期值）
- vendorFixDate（日期值）
- workaround（字符串值）
- solution（字符串值）

新的 BDSA 自动修复设置 (Beta)

当 Black Duck Security Advisory (BDSA) 团队分析 CVE 漏洞时，他们会检查受该漏洞影响的组件版本。有时，他们发现该漏洞适用于不同的版本集。如果 BDSA 团队发现该漏洞不适用于该组件版本，这个新功能将使您能够自动忽略 CVE 漏洞。这只会影响“新”状态的漏洞。

BDSA 自动修复是一项 beta 功能， 默认情况下未启用。要启用此功能，必须设置以下环境变量：

```
BDSA_AUTO_REMEDIATION=true
```

然后，可以在管理员 > 系统设置 > BDSA 自动修复页面上更改“BDSA 自动修复”设置。

注: 每当用户保存设置时，系统都会检查并可能更新所有项目的漏洞。在大型系统上，这可能需要很长时间，并对 Black Duck 性能产生影响。

已更新用户和组管理显示

“管理”>“用户和组”下的“用户”和“组”选项卡的观感已更新，通过将各个部分（“用户/组详细信息”、“总体角色”、“项目组”、“项目”、“用户/用户组”）细分为各自单独的页面，来更清晰地显示内容，从而更轻松地管理用户和组。

策略的新组件条件规则

未确认的代码段的新组件条件已添加。新的策略条件允许您创建或编辑策略，使您可以针对未审查的代码段触发策略违反。

新的软件材料清单 (SBOM) 报告 CycloneDX v1.3 导出格式

您现在可以用 CycloneDX v1.3 格式导出项目的软件材料清单报告。这可以通过查看项目版本，单击“报告”选项卡，单击“创建报告”按钮，然后选择 CycloneDX v1.3 - JSON 来完成。有关 CycloneDX v1.3 的更多信息，请访问 CycloneDX v1.3 参考页面。

“新的组件依赖关系重复敏感性” 系统属性

Black Duck 新增了一个系统属性，用于控制在软件包管理器扫描中添加到生成的依赖关系树中的每个组件的最大节点数（匹配）：

`blackduck.match.limit.per.component`

此系统属性的默认值为 10，因此树中的重复组件数不能超过 blackduck.match.limit.per.component 值（每个组件的匹配限制）。

支持的浏览器版本

- Safari 版本 15.4（16613.1.17.1.13，16613）
  - 不再支持 Safari 13.0 和更低版本
- Chrome 版本 100.0.4896.75（正式版本）(x86_64)
  - 不再支持 Chrome 版本 71 和更低版本
- Firefox 版本 99.0（64 位）
  - 不再支持 Firefox 版本 71 和更低版本
- Microsoft Edge 版本 100.0.1185.36（正式版）（64 位）
  - 不再支持 Microsoft Edge 版本 78 和更低版本

容器版本

- 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 增强

有关新增或更改的 API 请求的详细信息，请参阅 Black Duck 中提供的 API 文档。

项目端点的性能改进

发现以下 API 项目端点性能不佳并已进行优化：

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

修复了版本 2022.4.0 中的问题

在此发布中修复了客户报告的以下问题：

- (HUB-33047)。已修复一个问题，KbUpdateJob 过程中出现的“空指针异常”错误可能导致作业进度非常缓慢或看起来卡住。
- (HUB-32336)。将 BOM 页面上的“组件”过滤器重命名为“组件版本”，以使其与实际功能一致。
- (HUB-32316)。已修复一个问题，其中，在 docker 注册容器部署中，没有设置用于定义 JVM 的最大内存分配池的 HUB_MAX_MEMORY 环境变量。
- (HUB-32492)。已修复一个问题，其中，尽管在 BlackDuck 中 MIT 许可证设置为“已批准”，但具有 MIT 许可证的组件可能在快速扫描中触发“许可证未批准”和“许可证未审查”的策略违规。
- (HUB-31839)。已修复一个问题，其中，BDIO 上传端点项目和版本值未解码 URL。
- (HUB-32692, HUB-32672)。已修复一个问题，其中，如果某个组件有多个漏洞（每个漏洞的状态不同），除非该组件的所有漏洞都与所选的策略规则匹配，否则策略规则不会触发策略违反。
- (HUB-31872)。已修复一个问题，其中，快速扫描未验证用户权限。如果扫描找到匹配的项目版本 BOM，但用户没有权限 - 扫描将在没有项目版本或 BOM 组件数据的情况下运行。
- (HUB-33231)。已修复一个问题，其中，“扫描”页面上按扫描尺寸对扫描进行排序时，未按正确顺序显示列表。
- (HUB-33096)。修复了以下问题：按许可证系列过滤可能无法正确显示修改后的 KnowledgeBase 许可证。
- (HUB-30463)。修复了以下问题：Hub UI KnowledgeBase 搜索中未显示 golang.org/x/sys 组件。
- (HUB-31891)。已修复一个问题，其中，搜索“Apache HTTP 服务器”组件时，会链接到 debian 组件页面。
- (HUB-28406)。已修复一个问题，其中，某些 OSS 组件和版本中的“安全性”选项卡和“详细信息”选项卡有时会显示不同数量的漏洞。
- (HUB-32883)。已修复一个问题，其中，accessTokenValiditySeconds 设置的“最大存在时间”和“过期”字段与 JSON Web 令牌 (JWT) 的过期值不一致。
- (HUB-32313)。已修复 REST API /api/projects/<id>/versions/<id>/components 端点在处理高软件包管理器扫描数据负载时的性能问题。
- (HUB-32571)。修复了以下问题：在组件版本“版权”选项卡和 Black Duck 通知报告（以及“BOM 安全性”选项卡）中会不一致地显示来源名称空间。

- (HUB-32949)。已修复一个问题，其中，将用户直接分配给项目组，并将同一用户分配给也分配给项目组的用户组时，将导致 API 返回多个项目组，从而导致 Detect 失败。
- (HUB-33132)。已修复一个问题，其中，dependency-paths API 会消耗大量服务内存并分页到磁盘。
- (HUB-33155)。已修复一个问题，其中，HUB 注册刷新可能停止，这会导致 jobrunner 锁定时间变长，从而可能导致查询被阻止。
- (HUB-32010)。已修复一个问题，其中，在浏览“项目组”层次结构时，单击子组中的项目可能会将用户返回到根项目组。
- (HUB-32977)。已修复一个问题，其中，混合案例标记未按预期触发策略规则。
- (HUB-33305)。已修复 docker-compose.local-overrides.yml 文件中的缩进问题。
- (HUB-27940)。已修复一个问题，其中，部署到 EKS 时，如果没有指定最小 CPU 资源，Pod 将被分配 0.25 (250m) CPU 内核，导致 bomengine/rabbitmq 无法正常运行。
- (HUB-33455)。已修复一个问题，其中，连接到 CVE-2022-23395 的“漏洞详细信息”页面的链接将转到“404 未找到”错误页面。
- (HUB-32256)。修复了为自定义特征级别提交空值时会生成不正确的错误消息的问题。
- (HUB-32800)。已修复一个问题，其中，在 bitbake/yocto 扫描过程中，由于依赖关系树中每个组件的匹配数量非常大，导致 OutOfMemory 异常，matchengine 可能重启或作业在 jobrunner 中挂起。有关更多详细信息，请参阅上述“新增功能和更改功能”部分中的“新的组件依赖关系重复敏感性”系统属性项。
- (HUB-33349)。已修复一个问题，其中，默认情况下，webapp 容器需要一个名为“{{ .Release.Name }}-blackduck-webapp”的持久性卷，其中“Release.Name”通常是“hub”，或者在部署时选择的另一个标签。此外，一些客户可能已通过在 webapp values.yaml 覆盖中配置 persistentVolumeClaimName 来配置自定义持久性卷名称。不再需要这些配置（持久性卷和持久性卷声明），可以安全地删除。
- (HUB-32678)。已修复一个问题，其中，默认 IP 扫描不支持 scan.cli 参数 --matchConfidenceThreshold 来过滤匹配组件。
- (HUB-29532)。已修复一个问题，其中，当发行版映像中的 rootfs 路径不是从根目录开始，而是从子目录开始时，Linux 发行版软件包匹配中断。

Black Duck SCA 2022.2.x

版本 2022.2.2 中的新增功能和更改功能

Black Duck 版本 2022.2.2 是维护版本，不包含新的功能或更改的功能。对联机帮助进行了修复以防止安全漏洞。

容器版本

- 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 增强

有关新增或更改的 API 请求的详细信息，请参阅 Black Duck 中提供的 API 文档。

修复了版本 2022.2.2 中的问题

在此发布中修复了客户报告的以下问题：

- (HUB-34065)。修复了 SPDX 验证工具中导致以下错误的 SPDX 2.2 报告格式：
  `########[################## {"pointer":"/packages/0"} # ["packageSupplier"]`

版本 2022.2.1 中的新增功能和更改功能

已更新数据删除功能 (Beta)

数据删除功能允许您探索根据定义的条件自动删除项目版本的方法。对于存在版本限制、磁盘空间限制或数据库瓶颈的用户，过时版本的累积可能会对其过程或系统性能造成问题。如果随着时间的推移生成多个项目版本，且这些版本随着时间的推移而过时，此功能将非常有用。

在 Black Duck 2022.2.0 中添加，添加了一个新的环境变量：

- `BLACKDUCK_AUTOMATIC_VERSION_REMOVAL_RELEASE_PHASES`
  - 定义哪些项目版本阶段适用于数据删除过程。
  - 版本阶段值包括：规划、开发、已发布、已弃用、已存档和预发布
  - 如果未设置，默认值为“开发”。
  - 值不区分大小写。
  - 可以添加多个版本阶段，阶段以逗号分隔。

已更新项目和项目组的角色分配

现在，您可以将用户添加到项目和项目组中作为“项目查看者”。将用户添加到项目或项目组时，现在会自动选择“项目查看者”角色，并用作默认角色。然后，您可以根据需要向用户添加更多角色。

已更新最小扫描间隔配置

从 Detect 7.13 和更高版本开始，针对“最小扫描间隔”的 Black Duck Hub 扫描设置将被禁用。最小扫描间隔应通过 Detect 以命令参数的形式配置，如下所示：

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

其中 ## 是时间（小时）。

容器版本

- 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 增强

有关新增或更改的 API 请求的详细信息，请参阅 Black Duck 中提供的 API 文档。

修复了版本 2022.2.1 中的问题

在此发布中修复了客户报告的以下问题：

- (HUB-32540)。已修复 KbUpdateJob 的一个罕见问题，其中，重复值插入可能会减慢作业速度或使作业失败。
- (HUB-32544)。已修复一个竞态条件问题，其中，KbUpdateJob 试图插入一个已经被扫描插入的 version_bom_component。
- (HUB-33045)。已修复一个问题，其中，专门为快速扫描创建策略规则时，可能导致所有项目版本进入重新计算状态，BOM 的状态将更改为 “正在处理” 。
- （HUB-32363 和 HUB-33027）。已修复在取消映射以下方案的代码位置时可能出现的竞态条件（不使用 --detect.project.codelocation.unmap=true）：
  - 重新扫描代码位置并将其映射到其他项目版本。
  - 从 UI 手动取消映射代码位置。
  - 从 UI 手动删除代码位置。
  - 代码位置由 ScanPurgeJob 删除。

- (HUB-33155)。已修复一个问题，其中，HUB 注册刷新可能停止，这会导致 jobrunner 锁定时间变长，从而可能导致查询被阻止。
- (HUB-33132)。已修复一个问题，其中，dependency-paths API 会消耗大量服务内存并分页到磁盘。
- (HUB-31212)。已修复一个问题，其中，一个子项目组的成员可以访问所有项目组及其树。
- (HUB-33162)。已修复一个问题，其中，当设置的最高优先级安全风险排名与漏洞类型（BDSA 与 NVD）和 CVSS 首选项不匹配时，快速扫描中的漏洞结果可能显示错误的信息。
- (HUB-31756)。已修复一个问题，其中，“项目查看者”和“项目组查看者”角色无法分配给添加到项目和项目组的用户。
- (HUB-33047)。已修复一个问题，KbUpdateJob 过程中出现的“空指针异常”错误可能导致作业进度非常缓慢或看起来卡住。

版本 2022.2.0 的公告

增强型特征生成

从 Black Duck 2022.2.0 版本开始，Signature Scanner 将默认在客户端而不是服务器上生成特征。

如果您使用的是 Blackduck 托管服务，或者您使用的是版本中包含的 Helm 图表或 Docker Swarm ‘yaml’ 文件，则此更改将无缝进行，无需您采取任何措施。您的服务不会受到任何干扰。

但是，如果您已经自定义了您的 Helm 图表或使用覆盖文件，请参阅我们社区页面上提供的再平衡指南，以获得更多信息帮助您完成过渡。

API 请求的最大页数限制

为了更好地管理系统资源，我们对某些 API 请求进行了最大页数限制。最大页数限制将设置为 1000 页，未来的 Blackduck 版本可能会更改。有关 2022.2.0 版本中受影响的 API 请求的列表，请参阅下面的“API 增强”一节。

已弃用的 API

在 Blackduck 2022.2.0 中，/cpes/{cpeId}/variants 端点将被弃用，取而代之的是 /cpes/{cpeId}/origins。/cpes/{cpeId}/variants 将在 Blackduck 2022.4.0 中删除。/api/cpes 元数据中的 API 链接也已更新以返回 /api/cpes/{cpeId}/origins 而不是 /api/cpes/{cpeId}/variants。

即将对资源指导进行的更改

在即将发布的 Black Duck 2022.4.0 版本中，将更新默认资源设置，并增加所有扫描卷的推荐设置。2022.4.0 版本将附带有关如何继续使用现有设置的说明。

请注意，确切的扫描吞吐量可能会因扫描大小、类型和成分而异。但是，我们在内部测试中使用了此细分来收集下表中的信息：

- 50% 完整特征扫描
- 40% 完整软件包管理器扫描
- 10% 开发者软件包管理器扫描

文件组织更改

除上述更改外，从 2022.4.0 开始，资源覆盖 YAML 文件的组织也将发生变化。

对于 Kubernetes，Helm 图表中的资源覆盖 YAML 文件的组织将发生变化。

- values 文件夹将被重命名为 sizes-gen01。

- 之前的 4 个 T 恤尺寸文件（small.yaml 等）将被移至新的 sizes-gen02 目录中。
- 新目录 sizes-gen03 将包含下表中命名的每个配置的资源覆盖文件；这些文件被命名为 10sph.yaml、120sph.yaml 等。

对于 Swarm，Black Duck 将不再直接在 docker-compose.yml 中分配容器资源。相反，资源将在单独的覆盖文件中指定。当前资源分配将移至 sizes-gen02/resources.yaml。对于 Black Duck 2022.4.0 及更高版本，将在 sizes-gen03 folder 中提供多个可能的分配。

对于 Kubernetes 和 Swarm，将根据测得的负载即每小时平均扫描数进行 7 次分配；如果您的预期负载与其中一个预定义的分配不匹配，请对其进行取整。例如，如果预计每小时扫描 100 次，请选择 sizes-gen03/120sph.yaml。

资源指导和容器可扩展性

这些设置将应用于 Kubernetes 和 Swarm 安装。

名称	扫描次数/小时	Black Duck 服务	PostgreSQL	总数
10sph	10	CPU：10 核 内存：29 GB	CPU：2 核 内存：8 GB	CPU：12 核 内存：37 GB
120sph	120	CPU：12 核 内存：46 GB	CPU：4 核 内存：16 GB	CPU：16 核 内存：62 GB
250sph	250	CPU：16 核 内存：106 GB	CPU：6 核 内存：24 GB	CPU：22 核 内存：131 GB
500sph	500	CPU：27 核 内存：208 GB	CPU：10 核 内存：40 GB	CPU：37 核 内存：249 GB
1000sph	1000	CPU：47 核 内存：408 GB	CPU：18 核 内存：72 GB	CPU：65 核 内存：480 GB
1500sph	1500	CPU：66 核 内存：593 GB	CPU：26 核 内存：104 GB	CPU：92 核 内存：697 GB
2000sph	2000	CPU：66 核 内存：593 GB	CPU：34 核 内存：136 GB	CPU：100 核 内存：729 GB

PostgreSQL 设置

使用 PostgreSQL 容器的客户需要使用 ALTER SYSTEM 手动设置值，而对 shared_buffers 的更改将在下一次重新启动 PostgreSQL 后才会生效。这些设置将应用于 Kubernetes 和 Swarm 安装。

名称	扫描次数/小时	PostgreSQL CPU/内存	shared_buffers (MB)	effective_cache_size (MB)
10sph	10	CPU：2 核 内存：8 GB	2654	3185
120sph	120	CPU：4 核 内存：16 GB	5338	6406
250sph	250	CPU：6 核 内存：24 GB	8018	9622
500sph	500	CPU：10 核 内存：40 GB	13377	16053

1000sph	1000	CPU：18 核 内存：72 GB	24129	28955
1500sph	1500	CPU：26 核 内存：104 GB	34880	41857
2000sph	2000	CPU：34 核 内存：136 GB	45600	54720

日语

2021.10.0 版本的 UI、联机帮助和发行说明已本地化为日语。

简体中文

2021.10.0 版本的 UI、联机帮助和发行说明已本地化为简体中文。

版本 2022.2.0 中的新增功能和更改功能

Logstash 更新

为解决 CVE-2021-44832 漏洞，Black Duck 中使用的 Logstash 映像已升级至 7.16.3，该版本使用 Log4j2 版本 2.17.1。

增强型特征生成

如公告中所述，特征扫描程序将默认在客户端而不是服务器上生成特征。

如果您使用的是 Blackduck 托管服务，或者您使用的是版本中包含的 Helm 图表或 Docker Swarm ‘yaml’ 文件，则此更改将无缝进行，无需手动操作。您的服务不会受到任何干扰。

但是，如果您已经自定义了您的 Helm 图表或使用覆盖文件，请参阅我们社区上提供的再平衡指南文章，以获得更多信息帮助您完成过渡。

您还可以在社区上找到有关使用 Prometheus 和 Grafana 监测 Black Duck 的更多信息。

快速扫描增强

使用相同的端点，但添加了一个新标头以接受快速扫描模式。新 HTTP 标头被命名为 'X-BD-RAPID-SCAN-MODE'，并接受以下值：

- ALL：默认操作。它将评估 RAPID 或（RAPID 和 FULL）的策略规则。当标头为空时（这是默认值）。
- BOM_COMPARE：将像 ALL 一样评估所有策略规则，但现在将根据策略规则模式的类型进行不同的评估。当策略规则为（RAPID 和 FULL）时，它的行为类似于 BOM_COMPARE_STRICT，但如果策略规则为仅 (RAPID)，则其行为类似于 ALL。仅是 RAPID 的策略将在结果中具有空策略状态。
- BOM_COMPARE_STRICT：只会评估（RAPID 和 FULL）的策略规则。肯定结果中的所有策略规则都将具有 NEW 或 RESOLVED 状态。将策略违规与现有项目版本 BOM 进行比较。如果策略违规在 BOM 中已知且可见（活动或被覆盖），则此策略违规不是快速扫描肯定结果的一部分，它仍是遵循现有限制的完整结果的一部分。

为了运行任一种 BOM_COMPARE 模式，HUB 中必须有一个现有的项目版本。

PostgreSQL 11 容器迁移

CentOS PostgreSQL 9.6 容器现已被 Blackduck PostgreSQL 11 容器取代。新 blackduck-postgres-upgrader 容器将数据库从 PostgresSQL 9.6 迁移到 PostgreSQL 11，并在完成后退出。

强烈建议使用非核心 PG 扩展的客户在迁移前卸载这些扩展，并在迁移成功完成后重新安装；否则，迁移可能会失败。

进行复制设置的客户在迁移之前需要遵循 pg_upgrade 文档中的说明。如果没有进行上述的准备工作，迁移可能会成功，但复制设置将会中断。

重要提示：开始迁移之前：

- 确保您有额外的 10% 磁盘空间，以避免由于系统目录的数据复制而导致磁盘使用情况出现意外问题。
- 检查根目录空间和卷安装以避免磁盘空间不足，因为这可能导致 Linux 系统中断。

使用 synopsysctl 更新到 2022.2.0 将执行以下任务：

- 停止 Black Duck 实例
- 为 Black Duck 提供的 PG 容器的用户运行数据库迁移作业
- 更新并重启实例

对于 Kubernetes 和 OpenShift 用户：

- 迁移由一次性作业执行：
  - 停止 Black Duck；例如，

    ```
    kubectl scale --replicas=0 -n <your_namespace> deployments --selector
     app=blackduck
    ```

  - 运行升级作业；例如：

    ```
    helm upgrade <your_deployment_name> .-n <your_namespace>
     <your_normal_helm_options> --set status=Stopped --set runPostgresMigration=true
    ```

  - 使用 helm upgrade 正常重启 Black Duck。
  - 此迁移将 CentOS PostgreSQL 容器的使用替换为 Black Duck 提供的容器。此外，synopsys-init 容器将替换为 blackduck-postgres-waiter 容器。
- 在普通 Kubernetes 上，升级作业的容器将以 root 身份运行。但是，唯一的要求是作业与 PostgreSQL 数据卷的所有者以相同的 UID 运行。
- 在 OpenShift 上，升级作业假定它将使用与 PostgreSQL 数据卷所有者相同的 UID 运行。

对于 Swarm 用户：

- 迁移完全是自动进行的；除了标准的 Black Duck 升级之外，不需要额外的操作。
- blackduck-postgres-upgrader 容器必须以 root 身份运行才能更改上述布局和 UID。
- 随后 Black Duck 重新启动时，blackduck-postgres-upgrader 将确定不需要迁移，并立即退出。
- 可选：成功迁移后，blackduck-postgres-upgrader 容器不再需要以 root 身份运行。

更新了安全风险排名

根据一般行业趋势，默认的安全风险排名现在使用 CVSS 3.0 评分作为主要得分指标，同时使用 BDSA 来提高漏洞评分的准确性。

新的默认排名是：

- BDSA (CVSS v3.x)
- NVD (CVSS v3.x)
- BDSA (CVSS v2)
- NVD (CVSS v2)

此更新只会更改新安装的排名。对现有实例的任何升级都应保持先前设置的排名顺序。

版本详细信息组件报告增强

新的组件链接列已添加到“版本详细信息组件报告”中。此列将包含查看组件详细信息页面时显示的组件 URL。通过在仪表板上选择所需项目、选择版本、单击“报告”选项卡、单击“创建”按钮，然后选择“版本详细信息报告”，即可生成此报告。在以下弹出窗口中，确保选中“组件”复选框以生成包含新“组件链接”列的组件报告。

漏洞警告显示增强

在查看项目中的组件漏洞时，如果有问题的漏洞具有与此项目版本使用的组件版本无关的链接 BDSA，Black Duck 立即会向您发出警告。查看指定的漏洞时将显示一条消息，说明以下其中一条消息。

如果 BDSA 漏洞没有关联的 NVD 记录：

> Black Duck Security Advisory (BDSA) 团队将 <vulnerability ID> 映射到此组件版本，但它未包括在国家漏洞数据库 (NVD) 的相关记录中。

如果 NVD 漏洞没有关联的 BDSA 记录：

> 国家漏洞数据库 (NVD) 将 <vulnerability ID> 映射到此组件版本，但 Black Duck Security Advisory 团队已确定它不受影响。

有关 BDSA 漏洞的详细信息，请参阅 Black Duck 帮助文档。

基于 Jobrunner 堆和 CPU 的限制

从 Blackduck 2022.2.0 开始，jobrunner 容器将监测其堆和 CPU 使用情况，并可以根据当前资源使用情况减少其工作量。例如，如果堆使用量超过 90%，则 jobrunner 可以自行暂停，直至内存资源恢复。当资源可用时，jobrunner 将根据可用资源的比例增加其工作量。

如果 jobrunner 自行暂停，它将显示在“管理员”>“诊断”>“系统信息”>“jobruntime”页面上。您将看到一个条目，例如：

> 1 个活跃的 job runner 端点：
>
> docker-swarm_jobrunner_1.docker-warm_default/58993e70a84c(172.23.0.15), paused=true

"paused=true" 表示由于资源限制，该 jobrunner 不再执行任何其他操作。资源利用率一旦恢复，条目将更改为 paused=false，jobrunner 将开始承担新的工作。

来源报告中忽略的代码段

现在，您可以将环境配置为在您的来源报告中包含忽略的代码段。这可以通过设置环境变量 INCLUDE_IGNORED_COMPONENTS_IN_REPORT=TRUE 来完成。

组件搜索版本计数增强

现在，在搜索要添加到项目中的组件时，您可以看到特定组件的版本数量。当您键入组件名称时，计数将动态显示在搜索结果中。

安全漏洞修复增强

为了防止在尝试更改项目的修复状态时出现混淆，已对安全漏洞的修复过程进行了明确说明。当查看项目中的安全漏洞时，您可能会看到已散列且无法选择进行修复的行。这是由于该项目具有链接的安全漏洞记录类型（BDSA 或 CVE）。如果该漏洞未在“安全风险排名”中列为优先，则无法为该项目实施修复计划。切换到优先处理的安全漏洞记录将允许您更新该项目的修复计划。

项目版本克隆增强

现在，您可以在克隆项目版本时包含深度许可证数据。这可以通过在仪表板上选择一个项目，并在查看项目版本时单击“设置”选项卡来完成。

按项目标记搜索

现在，您可以在“查找”页面上按标记搜索和选择项目。这允许为按标记分组的项目创建已保存的搜索 — 支持项目的仪表板，这些项目可能位于由标记标识的通用应用程序中。

策略的新漏洞条件规则

漏洞 ID 的新策略条件已添加。新的策略条件允许您创建或编辑策略，使您可以针对特定漏洞（CVE 或 BDSA）ID 来标记组件。

新的软件材料清单 (SBOM) 报告 SPDX 格式

您现在可以用 SPDX 格式导出项目的软件材料清单报告。这可以通过查看项目版本，单击“报告”选项卡，然后单击“创建报告”按钮来完成。我们目前支持 SPDX 2.2，并计划在更高版本的 Blackduck 中支持其他格式。

增强的特征扫描请求量管理

为了更好地管理增强型特征扫描在特定时间段内可能出现的更高请求量，扫描服务现在将返回 HTTP 429（太多请求量）错误，如果扫描服务达到最大操作限制，客户端将处理该错误。客户端将以 30 秒为增量重试 10 分钟，然后再声明扫描失败。

“查找”页面上的新排序选项

现在，可以在“查找”页面上按项目组对项目进行排序，从而更轻松地搜索分配给组织内特定项目组的项目。

/api/search/project-versions 的新 projectGroupMembership 筛选器

使用此筛选器将返回所有项目版本，这些项目版本是给定项目组的派生项，并匹配其他筛选器中指定的条件。projectGroupMembership 筛选器将仅返回用户有权访问的项目组。用法示例：/api/search/projectversions?filter=projectGroupMembership:PG~{projectGroupId)。

报告数据库增强

添加了一个新视图，该视图已添加到报告架构中：

- reporting.scan_view

Blackduck 与身份提供商 (IdP) 之间的安全通信

Blackduck 现在将创建一个有效期为 5 年的自签名证书，用于签署 SAML 身份验证请求。管理员可以通过转至“管理员”>“系统设置”>“用户身份验证”，在外部身份验证部分中选择“SAML”，然后选中发送签名的身份验证请求复选框来配置请求是否需要签名。

此选项的默认设置为未选中或不需要。启用后，将提供一个下载 Blackduck 公共证书的链接，并将其分发给用户，以供其 IdP 验证身份验证请求。

将不匹配的组件分配给已知组件

现在可以将 BOM 扫描期间发现的不匹配组件分配给已知组件。

新快速扫描组件依赖关系树

我们现在将在快速扫描输出中显示项目中易受攻击组件的所有实例的依赖关系树。这将使您能够清楚地看到其他参考组件或子项目等如何参考该组件。具有三个父依赖项的 jackson-core 组件的快速扫描输出示例：

"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"

]

] ,

已更新的项目组角色名称

已通过删除“项目组”字样更新了与项目组关联的角色的名称。此更新未更改角色的功能。有关角色的更新方式，请参见下面的列表。

- 项目组经理 → 项目经理
- 项目组安全经理 → 安全经理
- 项目组 BOM 注释者 → BOM 注释者
- 项目组 BOM 经理 → BOM 经理
- 项目组项目代码扫描者 → 项目代码扫描者
- 项目组策略违反审核者 → 策略违反审核者
- 项目组查看者 → 项目查看者

项目和项目组管理增强

现在，您可以更轻松地将多个用户和项目组添加到项目和项目组中。下拉菜单已增强，允许在单个添加用户或项目组交互中进行多项选择。

Logstash 容器内存增加

由于内存不足问题可能导致系统崩溃或重新启动，因此我们将分配给 Logstash 容器的内存从 1024M 增加到 2560M。这将会减少影响您操作的 webapp 中断次数。

项目组删除增强

现在，如果在任何现有策略规则表达式中引用了项目组，则无法再删除该项目组。

在搜索字符串时添加了新的扩展名

以下扩展名已添加到我们允许搜索字符串的扩展名列表中，以保持扩展名与知识库中 FLLD/FLCD 扫描的兼容性。

- pkginfo

- properties
- pc

支持的浏览器版本

- Safari 版本 15.0（16612.1.29.41.4，16612）
  - 不再支持 Safari 13.0 和更低版本
- Chrome 版本 94.0.4606.71（正式版本）(x86_64)
  - 不再支持 Chrome 版本 71 和更低版本
- Firefox 版本 92.0.1（64 位）
  - 不再支持 Firefox 版本 71 和更低版本
- Microsoft Edge 版本 94.0.992.38（正式版本）（64 位）
  - 不再支持 Microsoft Edge 版本 78 和更低版本

容器版本

- 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 增强

有关新的或更改的 API 请求的详细信息，请参阅 Blackduck 中提供的 API 文档。

新签名的身份验证请求字段

下面的 API 请求中添加了一个新 sendSignedAuthenticationRequest 字段，用于确定 Blackduck 是否应该向 IdP 发送签名身份验证请求。此字段的默认值为 FALSE。只有将“签名的身份验证请求”配置设置为 TRUE 时，下载证书的元链接才可用。

- `GET#POST /api/sso/configuration`

新 /api/active-users 端点

此新查询将返回自提供日期以来登录系统的用户的所有用户上次登录信息。此查询采用与休眠用户相同的 sinceDays 查询参数。

新项目版本报告端点

添加了以下公共端点以支持所有版本报告，无论其类型如何（通知文件、版本报告、漏洞修复、漏洞状态、漏洞更新、软件材料清单报告）：

- `GET /api/projects/{projectId}/versions/{projectVersionId}/reports`
- `GET /api/projects/{projectId}/versions/{projectVersionId}/reports/{reportId}`
- `DELETE /api/projects/{projectId}/versions/{projectVersionId}/reports/{reportId}`
- `GET /api/projects/{projectId}/versions/{projectVersionId}/reports/{reportId}/contents`
- `GET /api/projects/{projectId}/versions/{projectVersionId}/reports/{reportId}/download`

新策略规则公共端点

已添加了新的公共 API 请求以检索活动策略规则：

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

新 /api/cpes/{cpeId}/origins 端点

在 Blackduck 2022.2.0 中，/api/cpes/{cpeId}/variants 端点将被弃用，取而代之的是 /api/cpes/{cpeId}/origins。/api/cpes/{cpeId}/variants 将在 Blackduck 2022.4.0 中删除。/api/cpes 元数据中的 API 链接也已更新以返回 /api/cpes/{cpeId}/origins 而不是 /api/cpes/{cpeId}/variants。

API 请求的最大页数限制

以下 API 请求现在具有最大页数限制，以便更好地调节系统资源使用量。该限制当前设置为 1000 个项目。

- `GET /api/projects/<id>/versions/<id>/components`
- `GET /api/projects/<id>/versions/<id>/vulnerable-bom-components`
- `GET /api/codelocations`
- `GET /api/projects/<id>/versions`
- `GET /api/projects`
- `GET /api/users`

API 端点的新排序筛选器

名为 parentProjectGroupName 的新排序选项可用于以下 API 端点。这将允许按父项目组名称对项目版本进行排序。

- `/api/search/project-versions`
- `/api/watched-projects`
- `/api/dashboards/users/{id}/saved-searches/{id}`

新 GET /api/scan-readiness API 端点

已添加新的公共 API 端点，它提供所有扫描容器的准备状态。

- `GET /api/scan-readiness`

样例响应：

```
{
 "readiness": "ACCEPTING",
 "items": [
  {
   "id": "9dc7653a462b",
   "service": "scan",
   "readiness": "ACCEPTING",
   "updatedAt": "2021-12-21T17:26:01.495Z",
   "versionId": 1
  }
 ]
}
```

- 在多扫描副本环境中，如果所有扫描容器副本都运行良好，则聚合状态将为 ACCEPTING。系统可以顺利地接受和处理新扫描。
- 在多扫描副本环境中，如果一个扫描容器运行不正常，而其他副本运行良好，则聚合状态将为 PARTIAL。在这种状态下，系统将会过载。扫描性能可能会降低。扫描稍有可能会超时或失败。
- 在多扫描副本环境中，如果所有扫描容器都运行不正常，则聚合状态将为 DEGRADED。系统过载，无法接受新扫描。如果设置为“拒绝”，则不会接受新的扫描请求，并将发回 HTTP 429 返回码。
- 如果容器出现故障，则其条目将在 5 分钟后删除（时间间隔可配置）。

更新了 GET /api/codelocations/{codeLocationId}/scan-summaries 响应

在为 /api/codelocations/{codeLocationId}/scan-summaries 生成的 API 响应中找到的 scanType 值现在将拆分为不同的类型，以避免歧义。新值现在包括：

- `PACKAGE_MANAGER`
- `###`
- `BOM_IMPORT`
- `SIGNATURE`

传统扫描仍将 BDIO 用于 scanType 值。

请注意，此更改是在 Black Duck 2021.8.0 中引入的。

修复了版本 2022.2.0 中的问题

在此发布中修复了客户报告的以下问题：

- (HUB-31267)。修复了没有任何全局角色的用户可以通过扫描页面或直接通过项目 URL 访问所有项目的问题。没有扫描权限的用户现在将无法看到 projects/.../versions/.../codelocations 屏幕上的“上传扫描”按钮。
- (HUB-31734)。修复了“组件”页面上的筛选器对项目级用户不起作用的问题。
- (HUB-31993)。修复了如果上传的 BDIO 文件的版本/发布为空值时，扫描可能失败的问题。如果缺少版本/发行值，扫描将不会失败。
- (HUB-31964)。修复了由于 JDBC 查询参数过多而导致项目版本的 VersionReportJob 失败，从而无法生成某些报告的问题。

- （HUB-30479、HUB-31842）。修复了在使用非优先级漏洞记录进行修复时，使用 BDSA 和 CVE 记录的漏洞修复不起作用的问题。为了修复漏洞，必须使用优先级漏洞记录类型。
- (HUB-31207)。修复了在存档项目下的漏洞已修复但无法在应用后更新安全风险计数的问题。用户无法修复存档项目版本的漏洞，因此现在，在存档项目版本时，用于漏洞修复的“更新”按钮将呈灰色显示。
- (HUB-32029)。修复了重新扫描后某些“已忽略”组件可能变为“未忽略”组件的问题。
- (HUB-31768)。修复了在生成通知文件时，错误地包含了基于忽略代码段的版权的问题。
- （HUB-32296、HUB-32255）。修复了 REST API GET /api/vulnerabilities/CVE-2021-44228/affected-projects 返回 0 个项目的问题。另请注意，搜索结果和端点中的受影响项目计数现在也将计算具有相关漏洞的组件。
- （HUB-31801、HUB-32424）。修复了版权的“刷新”按钮出现在超级用户角色中的问题。此功能现在仅对有权更新版权的角色显示。
- (HUB-32692)。修复了下述问题：如果某个组件有多个漏洞（每个漏洞的状态不同），除非该组件的所有漏洞都与所选的策略规则匹配，否则策略规则不会触发策略违反。
- (HUB-32357)。修复了用于处理组件、组件版本、许可证、NVD 漏洞和 BDSA 漏洞的知识库更新的 KnowledgeBase 活动作业问题。以前，如果出现任何错误/问题，则会退回到处理所有适用项目版本的单一更新。这可能会造成许多混乱，并降低数据库更新作业的速度。
- (HUB-32543)。修复了下述问题：如果通过分配这些角色关闭项目经理角色的设置，项目经理和项目组经理角色可能会覆盖策略并修复漏洞。现在，只有具有这些权限的项目经理或超级用户才能分配安全角色。
- (HUB-31129)。修复了一个问题：如果组件也有 BDSA 记录，则 Hub 中的项目版本报告（例如漏洞详细信息报告）将打印出包含 BDSA 记录的 CVE 漏洞的 URL。漏洞报告现在不会打印附加 BDSA 编号的 CVE 链接。
- (HUB-31044)。修复了使用带有错误自定义字段 ID 值的 API 设置策略之后无法正确显示策略屏幕的问题。
- (HUB-31753)。修复了 CollectScanStatsJob 作业可能需要比预期更长的时间来竞争，从而导致不必要的数据库膨胀的问题。
- (HUB-31663)。修复了 QuartzSearchDashboardRefreshJob 可能会遇到的问题：它试图调度此作业的多个实例，进而可能会导致对数据库的大量阻塞查询。
- (HUB-31862)。修复了在日语本地化中 BOM 注释者角色缺少翻译的问题。
- (HUB-31208)。修复了 IBM COS SDK For Java 2.10.0 组件在 BOM 和组件版本安全选项卡中显示为易受攻击，但“组件版本”页面未显示任何漏洞的问题。
- (HUB-31735)。修复了报告 (source.csv) 和“来源”页面之间代码段记录不一致的问题。如果忽略的代码段包含在报告中，则 INCLUDE_IGNORED_COMPONENTS_IN_REPORT 环境变量现在也将驱动。
- (HUB-31566)。修复了由于作业过度调度、内存不足问题和/或长时间运行作业而导致服务可能遇到数据库连接错误的问题。
- (HUB-31997)。更正了 json-schema v0.3.0 组件的漏洞信息。
- (HUB-32527)。修复了创建“通知文件报告”时，以下模式会显示错误的报告类型名称的问题。
- (HUB-31750)。修复了 BDSA-2021-0395 页面上的损坏链接。
- (HUB-31976)。修复了具有“管理用户”角色的用户无法在“项目版本扫描”页面中管理扫描的问题。
- (HUB-32566)。修复了用户无法将文件映射到 Apache Pulsar 组件的问题。
- (HUB-31201)。修复了无法将用户分配给仅具有项目（组）查看者角色的项目（组）的问题。
- (HUB-31251)。修复了删除自定义字段选项可能会破坏策略 API 的问题。
- （HUB-29676、HUB-32912）。修复了无法从“添加/编辑组件”对话框中选择某些组件版本的问题。

- (HUB-30847)。修复了当 webapp 容器以非 root 用户身份运行时，在 webapp-logstash pod 上生成了一个权限被拒错误，而导致其崩溃的问题。
- (HUB-31375)。修复了“项目概述”中的“上次更新”值和“查找”>“项目”中的“更新”值不匹配的问题。
- (HUB-30004)。修复了 OpenShift 环境中的权限问题，在该环境中，使用 Detect 成功进行二进制扫描可能会在 HUB 上生成空白 BOM。
- (HUB-32159)。修复了为自定义特征级别提交空值时会生成不正确的错误消息的问题。
- (HUB-32142)。修复了由于缺少权限而导致 RabbitMQ 无法在 Openshift 上安装的问题。
- (HUB-32216)。修复了当用户尝试覆盖组件的策略违反，而特定版本尝试撤消组件版本的策略违反时，结果没什么变化的问题。
- (HUB-32312)。修复了 KBUpdateWorkflow 作业“组件版本更新”饱和并耗尽内存，而无法提前时间戳的问题。
- (HUB-31916)。修复了在刷新 UI 页面之前项目设置更新 API 可能无法生效的问题。
- (HUB-30088)。修复了注销 SSO 帐户时不显示注销页面的问题。
- (HUB-32442)。修复了用于检索依赖路径的 API 查询所花费的时间比预期的时间要长得多的问题。
- （HUB-32538、HUB-32541）。修复了下述问题：kbUpdateJob 可能出现故障并退回到需要更长时间才能完成的精细更新。
- (HUB-32708)。删除了在 Black Duck 2021.10.0 中引入的统计查询，该查询需要很长时间才能执行，导致运行 PostgreSQL 11 的 Azure 系统整体运行缓慢。Microsoft 支持部门已经提出了这一问题，并正在调查此问题。其他安装不受此问题的影响。
- （HUB-32364、HUB-31606）。修复了下述问题：如果表中有超过 15 次扫描并且用户尝试批量删除它们，则扫描页面可能会冻结并失去响应。
- (HUB-32602)。修复了下述问题：ScanPurgeJob 进程可能会错误地导致通过 IP 代码路径完成的软件包管理器扫描的当前扫描状态更改为 FAILED。
- (HUB-31122)。修复了有时由于 ScanPurgeJob 进程在后台运行，而在 bomengine 中跳过扫描的问题。
- (HUB-30882)。修复了由于时区转换而导致报告中漏洞修复的目标日期/实际日期比输入日期早 1 天的问题。
- (HUB-32434)。修复了单击铃声图标以显示所有通知，然后单击已生成通知的项目名称时会生成错误的问题。
- (HUB-32027)。修复了日语本地化中对“传递依赖关系二进制”的错误翻译。
- (HUB-30788)。添加了新的端点以支持所有版本报告，无论类型如何。有关更多详细信息，请参阅上面的“API 增强”部分。
- (HUB-32843)。修复了日语本地化的项目版本页面“组件”选项卡中缺少“代码段”的翻译。
- (HUB-31964)。修复了由于 JDBC 参数过多而导致项目版本的 VersionReportJob 失败，从而无法生成某些报告的问题。
- (HUB-32393)。修复了下述问题：如果 BOM 中存在代码段匹配，在筛选结果时，上部视图有时不会读取安全/许可证/运维风险。
- (HUB-32604)。修复了将环境变量 BLACKDUCK_CORS_ALLOWED_ORIGINS_PROP_NAME 设置为通配符时，CORS 功能不起作用的问题。

Black Duck SCA 2021.10.x

版本 2021.10.3 的公告

Apache Log4J2 的安全公告（CVE-2021-45046 和 CVE-2021-45105）

Apache 组织发布了 Log4j2 组件的新版本 (2.17.0)，该版本解决了 2.15.0 和 2.16.0 版本中未修复的其他漏洞。

当日志配置使用具有上下文查找或线程上下文映射模式的非默认模式布局来使用 JNDI 查找模式制作恶意输入数据时，CVE-2021-45046 允许攻击者控制线程上下文映射 (MDC) 输入数据，从而导致拒绝服务 (DOS) 攻击。

CVE-2021-45105 允许控制线程上下文映射 (MDC) 输入数据的攻击者制作包含递归查找的恶意输入数据，使 StackOverflowError 终止进程，从而导致拒绝服务 (DOS) 攻击。

有关更多信息，请参阅 Apache 的 Log4j 安全漏洞页面。

正如 Black Duck 2021.10.2 版本所述，我们认为 Black Duck 的产品、服务和系统的曝光度有限。在我们已经接触到的风险范畴内，我们已经修复或正在修复这种情况。请继续关注我们的社区页面以获取更多更新内容。

版本 2021.10.3 中的新增功能和更改功能

Log4j 更新

Apache Log4j 2 Java 库已更新至 2.17.0，以解决严重的 CVE-2021-45046 和 CVE-2021-45105 漏洞。

Logstash 更新

Black Duck 中使用的 Logstash 映像已升级至 7.16.2，该版本使用 Log4j2 版本 2.17.0。

容器版本

- 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

修复了版本 2021.10.3 中的问题

此版本修复了以下问题：

- (HUB-32233)。为响应 CVE-2021-45046 和 CVE-2021-45105，已将 Log4j 升级至版本 2.17.0。
- (HUB-32295)。使用 Log4j 2.17.0 将 Bitnami Logstash 更新至 7.16.2 版。

版本 2021.10.2 的公告

Apache Log4J2 的安全公告 (CVE-2021-44228)

Black Duck 已注意到与名为 Log4Shell（或 LogJam）的开源 Apache Log4j 2 Java 库相关的安全问题，该库于 2021 年 12 月 9 日通过该项目的 GitHub 公开披露。此漏洞允许未经身份验证的远程代码执行，并影响 Apache Log4j 2 版本 2.0 到 2.14.1。有关详细信息，请参阅官方 CVE 发布。

根据我们目前所了解的情况，我们认为 Black Duck 的产品、服务和系统的曝光度有限。在我们已经接触到的风险范畴内，我们已经修复或正在修复这种情况。请继续关注我们的社区页面以获取更多更新内容。

另请参阅：https://www.blackduck.com/blog/zero-day-exploit-log4j-analysis.html

版本 2021.10.2 中的新增功能和更改功能

Log4j 更新

Apache Log4j 2 Java 库已更新至 2.15.0，以解决严重的 CVE-2021-44228 漏洞。

容器版本

- 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

修复了版本 2021.10.2 中的问题

此版本修复了以下问题：

- (HUB-32174)。为响应 CVE-2021-44228，已将 Log4j 升级至版本 2.15.0。

版本 2021.10.1 中的新增功能和更改功能

RestResponseErrorHandler 改进功能

RestResponseErrorHandler 现在可以更好地适应来自 KnowledgeBase 和网络中其他服务器的意外响应，从而使 Black Duck 功能更加可靠。

容器版本

- 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

修复了版本 2021.10.1 中的问题

在此发布中修复了客户报告的以下问题：

- (HUB-31129)。修复了一个问题：如果组件也有 BDSA 记录，则 Hub 中的项目版本报告（例如漏洞详细信息报告）将打印出包含 BDSA 记录的 CVE 漏洞的 URL。漏洞报告现在不会打印附加 BDSA 编号的 CVE 链接。
- (HUB-31293)。修复了升级到 2021.8.x 后 Python 传递依赖关系更改为直接依赖关系的问题。
- (HUB-31764)。修复了更新漏洞的修复状态时在 BOM 计算过程中导致空指针异常的问题。

- (HUB-30004)。修复了 OpenShift 环境中的权限问题，在该环境中，使用 Detect 成功进行二进制扫描可能会在 HUB 上生成空白 BOM。
- (HUB-31879)。修复了构建 BOM 阶段扫描可能卡住的问题。有关更多详细信息，请参阅上述“新增功能和更改功能”部分中的“RestResponseErrorHandler 改进功能”。
- (HUB-31896)。修复了重新扫描后通过公共 API 对 BOM 漏洞的修复更新不会继续生效的问题。
- (HUB-31753)。修复了 CollectScanStatsJob 作业可能需要比预期更长的时间来竞争，从而导致不必要的数据库膨胀的问题。
- (HUB-31663)。修复了 QuartzSearchDashboardRefreshJob 可能会遇到的问题：它试图调度此作业的多个实例，进而可能会导致对数据库的大量阻塞查询。
- (HUB-31755)。修复了生成项目版本报告时可能导致 VersionReportJob 由于循环项目结构而造成内存不足的问题。
- (HUB-31566)。修复了由于作业过度调度、内存不足问题和/或长时间运行作业而导致服务可能遇到数据库连接错误的问题。

版本 2021.10.0 的公告

增强型特征扫描

2021.10.0 版本中的特征扫描提供了与 2021.8.0 版本中的软件包管理器扫描相同的性能改进。这些改进的一个关键部分是重复 BOM 检测。通过使用此功能，如果特征扫描不会更改已与特定项目和版本关联的 BOM，则会绕过 BOM 计算。

此外，借助增强型特征扫描，JobRunner 不再在传入软件包管理器或特征扫描的处理过程中发挥作用。尽管运行增强型特征扫描不需要更多的系统资源，但可能需要对容器进行轻微的再平衡。请联系 Black Duck 支持人员，以帮助您了解是否需要再平衡。我们鼓励所有客户都这样做，以便充分利用这些改进的功能。

关于 Detect 7.4 和 Black Duck 2021.8.0 的说明

为了确保获得完整的功能和兼容性，Black Duck 版本 2021.8.0 需要使用 Detect 7.4。用户可以继续将旧版本的 Detect 与 Black Duck 配合使用，但在使用聚合的 BDIO 文件时，可能会在 BOM 中遇到不准确的依赖类型或来源视图。

升级到 Detect 7.4 可确保您避免 BOM 中的这些不准确问题。

PostgreSQL 容器从 9.6 迁移到 11

Black Duck 在 2022.2.0 版本中，将其 PostgreSQL 映像从版本 9.6 迁移到版本 11。不使用 Black Duck 提供的 PostgreSQL 映像的客户不会受到影响。

Black Duck 弃用 PostgreSQL 9.6

正如 Black Duck 2020.6.0 版本中宣布的那样，Black Duck 将在 2021.6.0 版本中终止对外部 PostgreSQL 9.6 的支持。从 2022.2.0 版本开始，Black Duck 将不再使用 PostgreSQL 9.6，如果指向 PostgreSQL 9.6 实例，将无法启动。

PostgreSQL 支持时间表

从即将发布的 2022.10.0 版本开始，Black Duck 将终止对外部 PostgreSQL 11 的支持。请参阅下表，了解对未来 PostgreSQL 版本支持的开始和结束日期。

PG 版本	首次发布	最新发布	BD 外部支持添加	BD 外部支持结束
16.x	2023 年末	2028 年末	2024.10.0	2026.10.0

15.x	2022 年末	2027 年末	2023.10.0	2025.10.0
14.x	2021 年 9 月	2026 年 11 月	2022.10.0	2024.10.0
13.x	2020 年 9 月	2025 年 11 月	2021.8.0	2023.10.0
12.x	2019 年 10 月	2024 年 11 月	X	X
11.x	2018 年 10 月	2023 年 11 月	2020.6.0	2022.10.0

从 2021.10.0 版本开始弃用数据库 bds_hub_report

从 2021.10.0 版本开始，新安装的 Black Duck 将不再创建 bds_hub_report 数据库。我们计划在 2022.10.0 中最终删除 bds_hub_report。

此外，如果 bds_hub_report 不存在，hub_create_data_dump.sh 和 hub_db_migrate.sh 脚本（随我们的编排文件分发）将不再出现故障。

- 如果 bds_hub_report 存在，hub_create_data_dump.sh 脚本将转储它，但如果不存在，将不会出现故障。如果 bds_hub_report 不存在，脚本将显示一条消息，说明已跳过它。
- 如果 bds_hub_report 存在，则无论是否存在转储文件，hub_db_migrate.sh 脚本都会尝试恢复它（与以前版本的行为一致）。如果 bds_hub_report 不存在，脚本将不会尝试恢复它，也不会考虑是否存在转储文件。
- 如果用户希望将其 bds_hub_report 数据库从 2021.8.x 或更早版本传播到新安装的 2021.10.0 或更高版本，则会添加一个新脚本 hub_recreate_reportdb.sh 来重新创建 bds_hub_report。在这种情况下；
  - 在旧数据库实例上运行 hub_create_data_dump.sh。
  - 在新数据库实例上运行 hub_recreate_reportdb.sh。
  - 使用在步骤 1 中创建的转储文件，在新数据库实例上运行 hub_db_migrate.sh。

即将对 API 请求实施最大页面限制

从 Black Duck 2022.2.0 开始，将对 API 请求实施最大页面限制。用户应发出符合以下条件的单个请求：其中包含的限制请求参数小于或等于记录的页面限制。如果请求的页面超过记录限制，则会被截断，以仅返回最大可接受的页面限制。针对页面尺寸的请求不会被拒绝，但会返回每个页面请求的最大结果数。

这将是一项延续到后续版本的持续工作，以提高应用程序的稳定性，并防止因不合理的大量请求而导致性能下降。

已弃用的 API

现在，以下已失效的端点将返回“404 NOT FOUND”错误，以表明对目标资源的访问不再可用：

- GET /oauthclients
- POST /oauthclients
- DELETE /oauthclients/{oAuthClientId}
- GET /oauthclients/{oAuthClientId}
- PUT /oauthclients/{oAuthClientId}
- POST /vulnerabilities/vulndb-copy

日语

2021.8.0 版本的 UI、联机帮助和发行说明已本地化为日语。

简体中文

2021.8.0 版本的 UI、联机帮助和发行说明已本地化为简体中文。

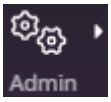
版本 2021.10.0 中的新增功能和更改功能

更新了有关增强型特征生成的错误消息

已更新了特征扫描服务器端的错误消息。在即将发布的版本中，用户指南中将提供完整的错误消息列表。

未映射扫描数据保留配置设置

管理员现在可以使用新的配置设置来更改未映射扫描的默认保留期。从 Black Duck 2021.10.0 开始，默认情况下将启用此设置，并将其设为 30 天（以前为 365 天）。此保留设置可以进行更新，最短可以设置为 1 天，最长为 365 天。

要在 UI 中更改此设置，请单击 

，单击“设置”，然后单击“数据保留”。

估计安全风险

通过查看按安全漏洞严重性类别排序的组件的所有版本并计算每个组件版本的每种严重性类别的最大漏洞计数，可以得出此估计风险统计。每种严重性类别的最大漏洞计数显示在安全风险物料清单上的“按严重性类别估计的安全风险”中。最高严重性类别计数可能参考不同的组件版本。例如：

- 版本 1.1 有 2 个严重漏洞，3 个高风险漏洞，15 个中风险漏洞，4 个低风险漏洞
- 版本 1.2 有 2 个严重漏洞，4 个高风险漏洞，12 个中风险漏洞，1 个低风险漏洞
- 对于未知版本的组件，按严重性类别估计的安全风险将在物料清单上返回 2 个严重漏洞，4 个高风险漏洞，15 个中风险漏洞，4 个低风险漏洞。

用户应选择应用程序中使用的准确版本，以查看准确的风险，而不是估计的风险。提供此估计风险信息的目的是帮助确定哪些组件需要首先审查。我们鼓励用户将估计风险信息与 BD 策略管理结合使用，以根据公司的安全策略进一步确定应优先考虑哪些组件。

注：所提供的信息只是统计数据估计。因此，估计的安全风险将没有 CVE 数据。

启用深度许可证数据时生成通知报告

现在，通知文件将在其他许可证之前放置任何已声明的许可证。然后，声明的许可证和其他许可证将按字母顺序排序。

在来源视图和来源报告中添加注释

现在，可以在项目的“来源”视图中为条目添加注释。文件注释还会显示在代码段视图中。这些注释还会显示在来源报告的名为“注释”的新列中。在“报告”选项卡中，选中版本详细信息报告的“来源”复选框，以创建来源报告。

您可通过以下方式在“来源”选项卡中为特定条目保留注释：

- 单击该组件行末尾的 图标，然后从下拉菜单中选择“注释”，或者单击 图标（如果已存在注释）。
- 单击“来源”视图中的条目，单击组件的“名称”，单击 图标，然后从下拉菜单中选择“注释”，或者单击 图标（如果已存在注释）。

策略管理增强 - 项目组

Black Duck 现在，用户能够对项目组及其子项应用策略规则。要执行此操作，请转至策略管理，然后单击创建策略规则按钮或 按钮，然后选择编辑。当 “创建/编辑策略规则” 模式打开时，请确保项目的子集，过滤方式...选项已启用，以查看 “项目条件” 过滤器下拉列表。

策略管理增强 - 为漏洞条件添加了远程代码执行 (RCE)

Black Duck 用户现在可以在创建或编辑策略时将远程代码执行 (RCE) 添加为过滤器选项。要执行此操作，请转至策略管理，然后单击创建策略规则按钮或 按钮，然后选择编辑。新的远程代码执行 (RCE) 值将显示在 “漏洞条件” 下拉菜单中。

对项目组经理权限的更改

以前，为了便于项目经理修复漏洞或覆盖策略，项目组经理的实际权限不受全局设置的影响。现在，项目组经理角色权限将根据 “项目经理角色” 设置进行调整。

特征扫描程序模拟运行更新

以前，在执行特征扫描程序模拟运行时，输出将生成一个 JSON 文件。从 Black Duck 2021.10.0 开始，生成的输出文件将采用 .bdio 扩展名，并且是一个 zip 文件。与传统特征扫描的模拟运行一样，它将继续在相同的目录下生成。

支持的浏览器版本

- Safari 版本 15.0（16612.1.29.41.4，16612）
  - 不再支持 Safari 13.0 和更低版本
- Chrome 版本 94.0.4606.71（正式版本）(x86_64)
- Firefox 版本 92.0.1（64 位）
- Microsoft Edge 版本 94.0.992.38（正式版本）（64 位）
  - 不再支持 Microsoft Edge 79 和更低版本

容器版本

- 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 增强

GET /api/project-groups 的权限修复

已对 GET /api/project-groups api 端点进行了以下修复：

- GET api/project-groups 将仅返回用户有权查看的项目组搜索结果。
- GET api/project-groups/<project group ID> 对于具有“超级用户”角色的用户，将返回 HTTP 200 OK，否则将返回 HTTP 403 FORBIDDEN 响应。

GET /api/users/{userId} 的权限更改

GET /api/users/{userId} 端点现在不再具有权限检查（以前需要 USERMGL_READ 检查）。

- GET /api/users/ 端点（列出所有用户）将继续通过 USERMGMT_READ 权限进行保护。
- 仍将提供 /api/projects/{projectId} API 中的项目所有者用户（无论用户的权限状态如何）。
- 仍将删除在 Black Duck 版本 2021.8.2 中添加到项目角色的 USERMGMT_READ 权限。

GET /api/project-groups 的新过滤器参数

添加了一个名为 exactName 的新过滤器参数，以帮助查找特定的项目组。如果为 true，exactName 过滤器将确保仅返回与 q 中的名称值匹配的项目组。项目组的搜索条件不区分大小写。如果没有匹配项，则不返回任何内容。此外，必须在 exactName 过滤器为 true 时指定 q 参数，否则不会返回项目组。

请参阅以下内容，了解如何在 /api/project-groups 请求中使用过滤器：

```
/api/project-groups?q=name:<project group name>&filter=exactName:true
```

改进了 CPE 支持 API

新增了三个公共 API：

- GET /api/cpes [需要搜索参数。返回匹配的 CPE ID]
- GET /api/cpes/{cpeId}/versions [返回与 CPE ID 匹配的组件版本]
- GET /api/cpes/{cpeId}/variants [返回与 CPE ID 匹配的组件来源]

Copyright 2.0 数据和新的传统端点

Black Duck 现在推出了使用现有端点（如下所示）的 Copyright 2.0 数据，以服务于这一新的版权数据。没有删除或添加任何响应字段。

```
GET /api/components/{componentId}/versions/{componentVersionId}/origin/{originId}/file-copyrights
```

我们将继续通过创建新的端点来提供 Copyright 1.0（也称旧版）数据：

```
GET /api/components/{componentId}/versions/{componentVersionId}/origin/{originId}/file-copyrights-legacy
```

注意：此新端点不能直接在 Black Duck UI 中使用，而只能直接通过公共 API 使用。此外，由于现有端点现在仍将返回 Copyright 2.0 数据，因此所有 Black Duck 客户（无论他们使用的版本如何）都会看到这些新数据。

通过公共 API 披露 lastScanDate

现在，以下 API 将在公共 API 响应中披露 lastScanDate：

- `GET /api/projects/{projectId}/versions/{projectVersionId}/bom-status`

修复了版本 2021.10.0 中的问题

在此发布中修复了客户报告的以下问题：

- (HUB-29413)。现在，在“添加组件”或“编辑组件”模式中搜索组件更加准确，并且更容易找到“自定义组件”。
- （HUB-26545 和 HUB-30185）。修复了以下公共 REST API 端点未按预期更新 componentModification、componentModified 和 componentPurpose 组件条件的问题。
  - `/api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}`
  - `/api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}`
- (HUB-30474)。修复了当用户无法访问某些项目时，“受影响的项目”页面上显示的计数与实际结果不匹配的问题。
- (HUB-30623)。修复了以下问题：许多客户端启动的错误通过记录堆栈跟踪导致了严重的日志流失，或者错误地以比实际更严重的日志级别进行日志记录。
- (HUB-30099)。修复了 KB 更新未能更新现有 BOM 漏洞状态的问题。如果当前状态不是用户或系统更新，则在修复状态变化时，BoM 组件版本漏洞修复（可在 BoM 安全视图中找到）现在将由 KB 更新作业进行更新。
- (HUB-29773)。修复了 /api/projects/<project ID>/versions/<version ID>/vulnerable-bom-components 端点响应时间超过预期的问题。现在，对于每个版本的 BOM 组件，该请求只包含一个许可证定义，因此缩短了响应时间。如果用户使用许可覆盖导入了 Protex BOM 表，则只会看到较少数量的结果。
- (HUB-26924)。修复了一个问题，现在当 SAML SSO 用户登录失败时会显示用户容易理解的错误消息。如果 SSO 配置错误，将显示一个错误页面以指明配置问题。如果用户在 HUB 中被禁用，则会显示一个错误页面，通知用户联系系统管理员或未经授权的页面。
- (HUB-31176)。修复了当修复状态与特定项目版本关联时，快速扫描策略评估未检查 BOM 状态的问题。
- (HUB-30808)。修复了在查看任何项目 BOM 表中组件的“其他字段”时，不返回“自定义字段管理”中“BOM 表组件”选项卡下创建的自定义字段的问题。在 BOM 组件上编辑自定义字段时，最多显示 100 个自定义字段。
- (HUB-30922)。修复了项目版本级别上的说明未显示的问题。此字段现在将显示在项目级别上使用的说明。
- (HUB-31482)。修复了 HUB 2021.6.2 之后 Snippet 确认页面上未显示许可证的问题。
- (HUB-31003)。修复了用户在尝试对漏洞执行批量修复时可能遇到 HTTP 500 内部服务器错误的问题。
- (HUB-31425)。修复了与以前版本的 HUB 相比，版本详细信息报告在启动时花费大量时间运行/完成查询的问题。
- (HUB-29598)。修复了组件页面上的“打印”按钮生成的 PDF 中的漏洞数由于栏太长而被挤出的问题。
- (HUB-30133)。修复了 helm 部署中 T 恤尺寸 ymls 的 webui 容器的 XL 部署拥有比大型部署更少内存的问题。webui 容器的内存限制在 x-large.yaml T 恤尺寸中增加到 1024 Mi。

- (HUB-28889)。修复了无法访问 RabbitMQ 时 BOM 引擎无法启动的问题。
- (HUB-30215)。修复了 BDSA-2020-1311 错误地报告可用解决办法的问题。
- (HUB-30857)。修复了漏洞的“受影响的项目”页面未包括显示项目中被忽略组件的漏洞，但在查找项目总数时包括了这些漏洞的问题。现在，项目总数中也未包括被忽略组件的漏洞。
- (HUB-30603)。修复了当项目的安全选项卡下的 BDSA 或 CVE 记录显示为灰色时，用户可以在该记录下看到整个注释的问题。
- (HUB-28753)。修复了 BomEngine 在 Docker 中创建时不接受 HUB_PROXY_PASSWORD_FILE 机密值并返回 407 AUTHENTICATION REQUIRED 错误的问题。
- (HUB-31483)。修复了策略违反模式中的策略覆盖日期和用户信息在日语本地化中显示不正确的问题。

Black Duck SCA 2021.8.x

版本 2021.8.8 中的新增功能和更改功能

Black Duck 版本 2021.8.8 是维护版本，不包含新的功能或更改的功能。对联机帮助进行了修复以解决 CVE-2022-30278，该漏洞可能允许未经身份验证的远程攻击者进行跨站点脚本攻击。

容器版本

- 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

修复了版本 2021.8.8 中的问题

已修复客户报告的以下问题：

- (HUB-32811)。修复了由于 JDBC 参数过多而导致项目版本的 VersionReportJob 失败，从而无法生成某些报告的问题。

版本 2021.8.7 的公告

Apache Log4J2 的安全公告（CVE-2021-45046 和 CVE-2021-45105）

Apache 组织发布了 Log4j2 组件的新版本 (2.17.0)，该版本解决了 2.15.0 和 2.16.0 版本中未修复的其他漏洞。

当日志配置使用具有上下文查找或线程上下文映射模式的非默认模式布局来使用 JNDI 查找模式制作恶意输入数据时，CVE-2021-45046 允许攻击者控制线程上下文映射 (MDC) 输入数据，从而导致拒绝服务 (DOS) 攻击。

CVE-2021-45105 允许控制线程上下文映射 (MDC) 输入数据的攻击者制作包含递归查找的恶意输入数据，使 StackOverflowError 终止进程，从而导致拒绝服务 (DOS) 攻击。

有关更多信息，请参阅 Apache 的 Log4j 安全漏洞页面。

正如 Black Duck 2021.8.6 版本所述，我们认为 Black Duck 的产品、服务和系统的曝光度有限。在我们已经接触到的风险范畴内，我们已经修复或正在修复这种情况。请继续关注我们的社区页面以获取更多更新内容。

版本 2021.8.7 中的新增功能和更改功能

Log4j 更新

Apache Log4j 2 Java 库已更新至 2.17.0，以解决严重的 CVE-2021-45046 和 CVE-2021-45105 漏洞。

Logstash 更新

Black Duck 中使用的 Logstash 映像已升级至 7.16.2，该版本使用 Log4j2 版本 2.17.0。

容器版本

- 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

修复了版本 2021.8.7 中的问题

已修复以下问题：

- (HUB-32233)。为响应 CVE-2021-45046 和 CVE-2021-45105，已将 Log4j 升级至版本 2.17.0。
- (HUB-32295)。使用 Log4j 2.17.0 将 Bitnami Logstash 更新至 7.16.2 版。

版本 2021.8.6 的公告

Apache Log4J2 的安全公告 (CVE-2021-44228)

Black Duck 已注意到与名为 Log4Shell（或 LogJam）的开源 Apache Log4j 2 Java 库相关的安全问题，该库于 2021 年 12 月 9 日通过该项目的 GitHub 公开披露。此漏洞允许未经身份验证的远程代码执行，并影响 Apache Log4j 2 版本 2.0 到 2.14.1。有关详细信息，请参阅官方 CVE 发布。

根据我们目前所了解的情况，我们认为 Black Duck 的产品、服务和系统的曝光度有限。在我们已经接触到的风险范畴内，我们已经修复或正在修复这种情况。请继续关注我们的社区页面以获取更多更新内容。

另请参阅：https://www.blackduck.com/blog/zero-day-exploit-log4j-analysis.html

版本 2021.8.6 中的新增功能和更改功能

Log4j 更新

Apache Log4j 2 Java 库已更新至 2.15.0，以解决严重的 CVE-2021-44228 漏洞。

容器版本

- 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

修复了版本 2021.8.6 中的问题

已修复以下问题：

- (HUB-32174)。为响应 CVE-2021-44228，已将 Log4j 升级至版本 2.15.0。

版本 2021.8.5 中的新增功能和更改功能

Black Duck 版本 2021.8.5 是维护版本，不包含新的功能或更改的功能。

容器版本

- 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

修复了版本 2021.8.5 中的问题

- (HUB-31482)。修复 Black Duck 版本 2021.6.2 之后代码段确认页面上未显示许可证的问题。
- (HUB-31663)。修复了 QuartzSearchDashboardRefreshJob 试图调度此作业的多个实例，进而导致大量阻塞查询的问题。

版本 2021.8.4 中的新增功能和更改功能

Black Duck 版本 2021.8.4 是维护版本，不包含新的功能或更改的功能。

容器版本

- 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

修复了版本 2021.8.4 中的问题

- (HUB-31425)。修复了与以前版本的 HUB 相比，版本详细信息报告在启动时花费大量时间运行/完成查询的问题。

版本 2021.8.3 中的新增功能和更改功能

报告数据库增强

在报告模式下将以下数据添加到了 scan_stats_view：

- scan_size

容器版本

- 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

修复了版本 2021.8.3 中的问题

在此发布中修复了客户报告的以下问题：

- （HUB-29959、HUB-30391 和 HUB-30397）。修复了一个问题：由于在准备材料清单时知识库发出 500 内部错误响应，导致扫描无法完成。
- (HUB-31047)。修复了在填充版本 BOM 组件页面时，UI 对后端进行重复调用，进而对数据库产生不必要压力的问题。
- (HUB-30074)。修复了以下问题：非常小的代码位置代码段扫描有时会在更新上传源信息之前完成，从而使上传的源看起来已丢失。

版本 2021.8.2 中的新增功能和更改功能

Black Duck 版本 2021.8.2 是维护版本，不包含新的功能或更改的功能。

容器版本

- 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

修复了版本 2021.8.2 中的问题

在此发布中修复了客户报告的以下问题：

- (HUB-31078)。记录了当 --reuse-values 标志用作安装/升级的一部分时，无法在 Kubernetes 中安装和升级到 Black Duck 2021.8 的问题。有关更多详细信息，请参阅 Helm 图表下的 REAME.md。
- (HUB-31086)。修复了 BOM 页面右上角的代码段框在少数项目版本中缺失的问题。
- (HUB-31156)。修复了具有项目级 BOM 经理角色且没有任何全局或整体角色的用户无法访问项目 BOM 的问题。

版本 2021.8.1 中的新增功能和更改功能

Black Duck 版本 2021.8.1 是维护版本，不包含新的功能或更改的功能。

容器版本

- 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

修复了版本 2021.8.1 中的问题

在此发布中修复了客户报告的以下问题：

- (HUB-31029)。修复了项目经理角色设置覆盖个人/组的超级用户角色的问题。
- (HUB-30808)。修复了在查看任何项目 BOM 表中组件的“其他字段”时，不返回“自定义字段管理”中“BOM 表组件”选项卡下创建的自定义字段的问题。
- (HUB-30655)。修复了没有超级用户角色的用户可在管理菜单中看到“项目组管理”选项的问题。
- (HUB-31077)。修复了以下问题：由于对 helm 图表中的属性进行更改，未能为 Kubernetes 部署将 Black Duck HUB 从 2021.6.0 升级到 2021.8.x。之前的其他版本不受影响。

版本 2021.8.0 的公告

Black Duck 2021.8.0 版本需要 Detect 7.4

Black Duck 2021.8.0 版本需要 Detect 7.4 才能运行。升级时，请确保满足最低版本要求。

CentOS-7 上的 Desktop Scanner

由于更新了依赖关系，最新版本的 Desktop Scanner 将无法在 CentOS-7 上运行。因此，专为 CentOS-7 测试版本创建了不同的 RPM，该版本将与旧版本的 Electron 12 一起运行。只要 Electron 12 受支持，我们将会一直维护这一独立 CentOS-7 测试版本。

除了我们当前的下载内容外，“工具”页面上还添加了一个链接，专门用于 CentOS-7 下载。常规 RPM、debian 软件包、macOS 和 Windows 安装程序照常提供。

日语

2021.6.0 版本的 UI、联机帮助和发行说明已本地化为日语。

简体中文

2021.2.0 版本的 UI、联机帮助和发行说明已本地化为简体中文。

已弃用的 API

以下端点已被移除：

- GET /api/scan/{scanId}/bom-entries

以下已失效的端点现在将返回“410 GONE”错误，以表明对目标资源的访问不再可用：

- GET /oauthclients
- POST /oauthclients
- DELETE /oauthclients/{oAuthClientId}
- GET /oauthclients/{oAuthClientId}
- PUT /oauthclients/{oAuthClientId}
- POST /vulnerabilities/vulndb-copy

版本 2021.8.0 中的新增功能和更改功能

对外部数据库的 PostgreSQL 13 支持

Black Duck 对于使用外部 PostgreSQL 的新安装，现在支持并建议使用 PostgreSQL 13。迁移到 2021.8.x 不需要迁移到 PostgreSQL 13。

内部 PostgreSQL 容器的用户无需执行任何操作。

请注意，PostgreSQL 12 不受支持。

安装文档将在即将发布的版本中更新。

Azure 客户通知

在 Azure PostgreSQL 13 完全发布之前，会尽最大努力支持 Azure PostgreSQL 13 上的 Black Duck，但不能保证分辨率。因此，我们强烈建议不要将 Azure PostgreSQL 13 用于生产部署，客户应该使用 Azure PostgreSQL 11。

有关 PostgreSQL 13 的 Azure 支持的更多信息，请访问 https://docs.microsoft.com/en-us/azure/postgresql/concepts-version-policy。

扫描的新系统设置：组件相关性复制敏感性

此设置允许用户更改系统如何为扫描期间在“来源”页面上找到的组件显示重复软件包 ID。在以前的版本中，作为 2021.8.0 中的默认设置（设置为 1），“来源”页面将只显示一个软件包 ID 发现，而不考虑在扫描中发现它的频率。将此设置更改为大于 1 将显示更多条目，从而可以更好地逐层查看，帮助确定每个组件源自哪个层。对于在启用 BOM 聚合的情况下在 Detect 中进行扫描、并希望查看已聚合到 1 次扫描中的各种模块中的软件包 ID 参考的客户，此功能尤其有用。

扫描的新系统设置：最小扫描间隔

此设置允许用户在使用 LCA 增强型特征扫描时更改在给定代码位置执行特征扫描的最小小时频率。默认设置设置为 0，或没有最小扫描间隔，这意味着不会阻止扫描发生，无论频率如何。如果设置为大于 0，则当特征扫描在设置的扫描间隔之前进行时，将不会处理特征扫描。例如，设置为 4 将不允许在 4 小时过去之前重新扫描特征。此设置可以在“管理”>“系统设置”>“扫描”页面中全局配置，也可以通过 Detect 客户端以命令行选项的形式进行配置。注意：仅当客户使用参数 --detect.blackduck.signature.scanner.arguments='--signature-generation' 进行扫描时，才使用此设置。

注: 启用此功能后，即使由于扫描间隔而未运行特征扫描，使用 Detect 执行的特征扫描也将完成并显示成功状态。日志中将显示一条警告消息，指示扫描未运行，但不会向用户提供其他指示。

“快速扫描”策略应用发生的更改

“快速扫描”的用户现在可以配置如何对完整（传统）扫描、快速扫描或两者的结果应用策略。从 2021.8.0 版开始，新安装的 Black Duck 的默认设置将设为仅应用于完整扫描。要使用快速扫描获取所有漏洞（无论策略如何），只需创建一个策略，设置条件严重性 >=0。

添加了完成的快速扫描次数的 phone-home 累计计数

此计数是准确的，数据不会丢失，但可能存在一些计时问题（一些扫描来自第二天的数据）。

策略管理中添加了快速扫描漏洞条件

策略管理中现在提供了以下漏洞条件：

- CWE ID
- 可用的解决方案
- 可用的解决方法
- 可用的漏洞利用
- 可从来源访问
- 修复状态

项目组管理

Black Duck 现在可以在 Hub 中对所有项目进行逻辑分组，使您可以整理出哪个项目属于哪个业务部门，从而能够更轻松地查看整个组织的风险。项目组可以同时包含项目和其他项目组，以提供多级层次结构。

用户和组可以分配给具有任意数量角色的项目组。该分配将授予这些用户对该组下具有指定角色的项目的访问权限，除非该分配在较低级别被明确覆盖。此概念允许设置对尚未创建的项目具备默认访问权限的用户。

此外，搜索仪表板已得到增强，能够返回用户可通过项目组访问的项目的搜索结果。

新的全局版本创建者、项目组 BOM 注释者用户角色以及对现有角色的更改

项目创建者和全局代码扫描者角色对“全局版本创建”权限的访问权限已被取消，将无法再创建他们不拥有或无法访问的项目的版本。对于依赖此功能的用户，为填补空缺，我们已设立了一个新的角色，即全局版本创建者。作为升级迁移脚本的一部分，所有具有项目创建者和/或全局代码扫描者的当前用户将自动继承此角色。这意味着，对于希望利用更细化的安全更改的当前用户，将明确选择退出此更改。

项目组 BOM 注释者对分配的项目组中的每个项目都具有 BOM 注释者权限。这意味着，他们可以为与项目组关联的项目添加或编辑注释并编辑自定义字段。

Protex BOM 工具令牌访问支持增强

Protex BOM 工具现在支持 BD_HUB_TOKEN 环境变量，以将从 Protex 导出的 json 上传到 Hub。您可以使用命令提示符通过添加“-T”来设置令牌。

将 BD_HUB_TOKEN=[insert token here] 变量添加到 .bash_profile 以使更改永久生效。

漏洞通知增强

添加了一个新的环境变量：在 blackduck-config.ev 文件中添加了 BLACKDUCK_NOTIFY_WHEN_REMEDIATED。它默认为 true，但在设置为 false 时，对于修复状态为“已忽略、修复完成、已缓解或已修补”的漏洞，Black Duck 将不再发送/创建“新”漏洞通知。

特征扫描超时消息增强

特征扫描期间的网络超时（等待来自 HUB 的响应）现在返回一条准确的错误消息，该消息指示网络超时，而不是 I/O 错误（代码 74）。新的消息格式将显示 Scan <Corresponding Scan ID> failed: [<Reason why it happened and whether to contact an administrator or retry the scan>]。

Black Duck Hub 增强功能的请求重试机制

已引入一个等候程序，当收到 HTTP 502/503/504 响应时，该等候程序将重试将扫描上传到 Hub。它将以 30 秒为增量重试 10 分钟，然后再声明扫描失败。

“扫描”页面增强

“扫描”页面中添加了一个新的“创建时间”列，允许您查看扫描创建的时间。使用“创建日期”选项筛选扫描时，列中显示的日期使用户可以更加轻松地比较日期。

显示无版本的组件的许可证风险信息

已引入新的逻辑来确定具有未知版本的组件的默认许可证。这是一个估计的许可证，基于它在组件的前 1,000 个版本中出现的最多次数。借助此许可证，您可以计算许可证风险，而无需选择版本。但是，建议您查看这些组件并手动指定版本以获得更准确的结果。

报告数据库增强

在报告模式下将以下数据添加到了 scan_stats_view：

- 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

策略规则条件增强

为策略规则“总体得分的漏洞条件类别”添加了一个新的策略条件运算符。现在，您可以在创建或编辑策略规则时选择“小于或等于”。

容器版本

- 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 增强

- 添加了新的 API，可启用代码段匹配的批量确认/取消确认和忽略/取消忽略。
  - `PUT /api/projects/{projectId}/versions/{versionId}/bulk-snippet-bom-entries ##### application/vnd.blackducksoftware.bill-of-materials-6+json`
- 以下 API 端点已更新，以考虑用户可以通过项目组成员资格访问的项目。查询参数也已从 name 更改为 entityName，以便与响应内容等同。
  - `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`

修复了版本 2021.8.0 中的问题

- (HUB-29341)。修复了使用 --include-files 标志从 Protex 导出 BOM 并将其导入到 Hub 实例时会生成 Java 堆空间错误的问题。
- (HUB-29005)。修复了以下问题：如果 BOM 具有两个名称完全相同但 UUID 不同的组件，则筛选器 API (/api/projects/projectId/versions/versionId/components-filters?filterKey=bomComponents) 应根据 ID 及其版本（如果存在）返回两个单独的组件，而不是按名称对它们进行分组。
- (HUB-29567)。修复了以下问题：在“项目版本”>“详细信息”视图中，“已更新”（或 2021.8.0 中的“上次设置更新”）时间戳会更新，但不会按用户名更新。“上次设置更新”时间戳和更新者用户名现在仅在更改项目版本详细信息时才会更新。
- (HUB-30139)。修复了 Protex BOM 工具中的问题，其中，使用 --include-files 标志时会出现 Unmarshalling 错误：非法字符。
- (HUB-12280)。修复了以下问题：如果上传的 BDIO 文件包含与项目之间的关系，当这些关系位于“BDIO 树”的较低层级时，这些关系在项目中不可见。
- (HUB-29481)。修复了以下问题：通知报告中省略了名称相同但大写字母不同的许可证。
- (HUB-30143)。修复了以下问题：Protex BOM 工具 2021.6.0 无法与最新 JDK (11.0.11) 配合使用。
- (HUB-29274)。修复了以下问题：当 BOM 页面上存在循环引用时，VersionReportJob 会导致 jobrunner 出现内存不足问题。
- (HUB-29381)。修复了以下问题：将项目版本添加为组件（使用“添加”>“项目”）时，组件条目会显示无效的运维风险级别。
- (HUB-30087)。修复了以下问题：当版本名称包含多字节字母数字字符时，项目版本查询无法找到版本。
- (HUB-23686)。修复了以下问题：对一个节点文件运行 Detect 时，特征扫描程序会卡住。
- (HUB-25592)。修复了以下问题：组件（或组件版本）的调整会自动从 BOM 中删除。
- (HUB-25552)。修复了以下问题：具有“MATCH”类型调整的组件（或组件版本）会自动从 BOM 添加/删除。
- (HUB-29196)。修复了以下问题：单击策略违规弹出窗口并将鼠标光标快速移离策略违规符号时，弹出窗口不会消失。
- (HUB-29573)。修复了以下问题：查看策略违规模式时忽略策略规则描述中的换行符。
- (HUB-30611)。修复了以下问题：数据库迁移脚本中的数字用户名会导致错误。
- (HUB-26611)。修复了以下问题：在 Detect 中使用聚合时无法正确报告直接/过渡依赖关系。请注意，此修复仅在使用 Detect 7.4 时得到解决，并且需要在 Detect 中使用新的子项目 detect.bom.aggregate.remediation.mode。

- (HUB-22379)。修复了一个性能问题：项目标记和设置标记策略在某些情况下可能需要耗费数小时时间。
- (HUB-30141)。修复了以下问题：Hub swarm docker-compose.yml 包含不受支持的“链接”选项。
- (HUB-29549)。修复了权限检查导致的 BOM 页面加载性能问题。

Black Duck SCA 2021.6.x

版本 2021.6.2 中的新增功能和更改功能

Black Duck 版本 2021.6.2 是维护版本，不包含新的功能或更改的功能。

容器版本

- 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

修复了版本 2021.6.2 中的问题

在此发布中修复了客户报告的以下问题：

- (HUB-30493)。修复了以下问题：由于在 NGINX 配置中指定了 Alert 的代理证书位置，托管用户无法访问 Blackduck Alert 实例。

版本 2021.6.1 中的新增功能和更改功能

Black Duck Security Advisory (BDSA) 远程代码执行风险

Black Duck 重点介绍了 2021.6.1 版本中可能允许远程代码执行 (RCE) 的漏洞。在 Black Duck UI 中，如果 BDSA 漏洞具有 RCE 标签，则它将出现在完整的 BDSA 记录、漏洞表以及特定组件的“安全”选项卡中。

漏洞 API 使用名为 bdsaTag 的阵列报告此漏洞。如果 bdsaTag 阵列包括“RCE”，则该漏洞可能允许远程代码执行。

- /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

容器版本

- 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

修复了版本 2021.6.1 中的问题

在此发布中修复了客户报告的以下问题：

- (HUB-29202)。修复了以下问题：增大超时和重试值后，2021.4.0 版的二进制扫描容器 (bdba-worker) 仍然无法在 Docker SWARM 环境中正常工作。
- (HUB-29405)。修复了以下问题：由于识别到 core_i7 架构，导致匹配项被丢弃。
- (HUB-30134)。修复了以下问题：由于 RabbitMQ 连接问题，导致 BOM 引擎无法静默启动。
- (HUB-30170)。修复了以下问题：使用双栈 Kubernetes 时，由于 docker-entrypoint 中的配置不正确，导致 Redis 无法启动。

- (HUB-30202)。修复了以下问题：当用户从 BDSA 评分切换到 NVD 评分时，漏洞详细信息页面无法正确地更改评分指标的显示，反之亦然。

版本 2021.6.0 的公告

对外部数据库已终止支持 PostgreSQL 版本 9.6

从 Black Duck 2021.6.0 发行版开始，对于外部数据库，Black Duck 已终止支持 PostgreSQL 版本 9.6。

Black Duck 对于外部数据库，现在将仅支持 PostgreSQL 版本 11.x。

已弃用的页面

如前所述，“扫描” > “组件” 页面已被移除。

已弃用的 API

以下端点已被弃用：

- GET /oauthclients
- POST /oauthclients
- DELETE /oauthclients/{oAuthClientId}
- GET /oauthclients/{oAuthClientId}
- PUT /oauthclients/{oAuthClientId}
- POST /vulnerabilities/vulndb-copy

日语

2021.4.0 版本的 UI、联机帮助和发行说明已本地化为日语。

版本 2021.6.0 中的新增功能和更改功能

新容器和系统要求的变更

在 2021.6.0 版本中：

- 添加了一个新容器 blackduck-webui，用于提高 Black Duck 性能、改进缓存和实现未来的可扩展性。
- 快速扫描功能已提供给所有 Black Duck 客户使用。此功能需要一个新的容器 blackduck-matchengine，该容器可管理与 Black Duck KnowledgeBase 的连接，并以较短的时间间隔缓存 KnowledgeBase 结果。

以下是现在运行所有容器的单个实例所需的最低硬件。请注意，内存要求取决于您要支持的并发快速扫描的数量。

- 7 个 CPU
- 28.5 GB RAM（最低 Redis 配置）；31.5 GB RAM（最佳配置），以便为 Redis 驱动的高速缓存提供更高的可用性。这将支持多达 100 个并发快速扫描。

  30 GB RAM（最低 Redis 配置）；33 GB RAM（最佳配置），以便为 Redis 驱动的高速缓存提供更高的可用性。这将支持超过 150 次快速扫描，但支持的快速扫描的最大数量仍待确定。
- 250 GB 可用磁盘空间，用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

以下是运行带有 Black Duck 二进制分析 的 Black Duck 所需的最低硬件。

- 8 个 CPU
- 32.5 GB RAM（最低 Redis 配置）；35.5 GB RAM（最佳配置），以便为 Redis 驱动的高速缓存提供更高的可用性。这将支持多达 100 个并发快速扫描。

  34 GB RAM（最低 Redis 配置）；37 GB RAM（最佳配置），以便为 Redis 驱动的高速缓存提供更高的可用性。这将支持超过 150 次快速扫描，但支持的快速扫描的最大数量仍待确定。
- 350 GB 可用磁盘空间，用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

注：每个附加的 binaryscanner 容器都需要一个额外的 CPU、2 GB RAM 和 100 GB 可用磁盘空间。

快速扫描

快速扫描现在可供所有客户使用。

Black Duck快速扫描为开发人员提供了一种方法，以快速确定项目中包含的开源组件版本是否违反了与使用开源组件有关的公司策略。通过使用 Black Duck Detect，快速扫描可以快速返回结果，因为它只使用软件包管理器扫描，并且不与 Black Duck 服务器数据库交互。当您需要快速反馈时，以及不需要在 Black Duck 中保留数据时，请使用快速扫描。

通过使用快速扫描，您可以运行数千次扫描，同时无需部署更多的 Black Duck 实例。它为您提供了可行的结果（比如构建失败），您可以在没有项目版本或无法访问 Black Duck 用户界面的情况下使用这些结果。

新的作业子系统

已用新的实施替换了作业子系统。

- 作业的可能状态现在可以是：
  - 待定
  - 进行中
  - 完成
  - 错误
- 您可以根据作业的时间表筛选作业：定期或按需。
- 在新的实施中，添加了以下作业：
  - BomAggregatePurgeOrphansCheckJob。检查是否有任何 BOM 数据与项目版本不相关，并启动必要的作业。
  - BomVulnerabilityDataRecomputationCheckJob。当某些设置发生变化时，检查是否需要进行 BOM 计算，并启动必要的作业。
  - BomVulnerabilityDataRecomputationJob。更新从 KnowledgeBase 收到的组件信息。
  - HierarchicalVersionBomCheckJob。检查是否需要分层 BOM 计算，并启动必要的作业来处理它们
  - JobHistoryStatsJob-计算每日统计。根据作业活动计算每日统计数据。
  - JobHistoryStatsJob-计算五分钟统计。根据作业活动，以 5 分钟间隔为周期计算统计数据。
  - JobHistoryStatsJob-计算小时统计。根据作业活动，以一小时为周期计算统计数据。
  - JobHistoryStatsJob-修整作业历史记录。根据保留设置，修整作业历史记录中的旧记录。
  - KBUpdateCheckJob。启动从 KnowledgeBase 收到的更新。
  - KbUpdateWorkflowJob-BDSA 漏洞更新。更新从 KnowledgeBase 收到的 BDSA 漏洞信息。

  - KbUpdateWorkflowJob-组件更新。更新从 KnowledgeBase 收到的组件信息。
  - KbUpdateWorkflowJob-组件版本更新。处理从 KnowledgeBase 收到的组件版本更新。
  - KbUpdateWorkflowJob-许可证更新。更新从 KnowledgeBase 收到的许可证信息。
  - KbUpdateWorkflowJob-NVD 漏洞更新。更新从 KnowledgeBase 收到的 NVD 漏洞信息。
  - KbUpdateWorkflowJob-Summary。发布关于最近的 KnowledgeBase 更新的总结报告。
  - LicenseTermFulfillmentCheckJob。检查是否需要处理许可证履行，并启动必要的作业。
  - NotificationPurgeCheckJob。检查是否有需要清理的通知，并启动必要的作业。
  - QuartzVersionBomEventCleanupJob。根据保留策略清理 BOM 事件。
  - VersionBomComputationCheckJob。检查是否需要 BOM 计算，并启动必要的作业来处理它们。
  - VersionBomNotificationCheckJob。发布 BOM 计算结果的通知。
  - WatchdogJob。监控重复作业，以确保其正常运行，并在确定问题后进行报告或修复。
- 以下作业已被移除：
  - KbUpdateJob

报告增强

- 已添加新的项目版本报告 license_conflicts_date_time.csv。它列出了此项目版本的许可证冲突。此报告包含以下列：
  - 组件 id
  - 版本 id
  - 组件名称
  - 组件版本名称
  - 用法
  - 许可证 id
  - 许可证名称
  - 来源/类型
  - 许可条款责任
  - 许可条款类别
  - 许可条款名称
  - 说明
  - 冲突的许可证 ID
  - 冲突的许可证名称
  - 冲突的许可条款来源类型
  - 冲突的许可条款责任
  - 冲突的许可条款类别
  - 冲突的许可条款名称
  - 冲突的许可条款描述

- components_date_time.csv 项目版本报告的末尾添加了一个新列“存在许可证冲突”。此列指示此组件版本是否存在许可证冲突。
- 报告的文件名现在使用系统时区，而不是 UTC。

刷新 Black Duck KnowledgeBase 版权信息的能力

Black Duck 现在您能够查看组件来源的经更新的 Black Duck KnowledgeBase 版权信息。如果有新的或更新的数据，Black Duck 会更新显示的信息，同时保留您所做的任何编辑。

新角色

Black Duck 中添加了一个新角色 BOM 注释者。具有此角色的用户具有项目的只读访问权限，可以在 BOM 中添加或编辑注释，并更新 BOM 自定义字段。

LDAP 或 SAML 组同步

如果在为 Black Duck 配置 LDAP 或 SAML 时启用了组同步，则外部身份验证系统（LDAP 或 SSO）中该组的名称现在将显示在组名称页面的外部组名称字段中。现在，如果外部系统上的组名称发生变化，您可以对其进行编辑，以使 Black Duck 组名称与外部身份验证系统组名称保持同步。

强制实施必填自定义字段

Black Duck 现在提供了一个选项，让用户在编辑具有必填自定义字段的对象时必须输入值。

用于项目搜索的新筛选器

Black Duck 现在在搜索项目时提供了以下筛选器：

- 从不扫描。使用此筛选器查找从未参与扫描的所有项目版本。
- 自...起未扫描。使用此筛选器查找自选定时间段以来尚未扫描的所有项目版本。

未映射的代码位置的保留期

未映射的代码位置的默认保留期已从 365 天更改为 30 天。

“添加/编辑组件”对话框中的其他信息

为了便于您更轻松地确定要使用的组件，“添加组件”和“编辑组件”对话框现在包括组件的主页 URL 和使用此组件的项目版本数。

策略增强

以下组件条件现在包括一个“false”选项：

- 许可证与项目版本冲突
- 未履行的许可条款
- 未知组件版本

改进了 C/C++ 匹配

在 2021.6.0 版本中，对于在 Linux 域中扫描 C/C++ 的客户，BOM 准确性已得到提高。

新的匹配类型

2021.6.0 版本中增加了两种新的匹配类型。

- 直接依赖关系二进制。可确定使用的二进制文件是直接依赖关系的扫描。
- 过渡依赖关系二进制。可确定使用的二进制文件是过渡依赖关系的扫描。

支持的浏览器版本

- Safari 版本 14.0.3（15610.4.3.1.7，15610）
- Chrome 版本 90.0.4430.72（正式版本）(x86_64)
- Firefox 版本 88.0（64 位）
- Microsoft Edge 版本 90.0.818.41（正式版本）（64 位）

容器版本

- 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

日语

2021.4.0 版本的 UI、联机帮助和发行说明已本地化为日语。

API 增强

- 更改作业子系统后：
  - GET /jobs/{jobID} 此调用按 ID 获取特定作业的作业详细信息。此调用现在将返回“404 Not Found”状态代码。
  - 以下调用自 Black Duck 版本 2020.2.0 起停止使用，将返回“404 Not Found”状态代码，并且在 Black Duck 版本 2021.6.0 中将保持无法使用：
    - PUT /jobs/{jobID} 此调用会重新安排作业。
    - DELETE /jobs/{jobID} 此调用会终止作业。

该功能将被新的作业 Rest API 实施所取代，该实施将在未来的版本中提供。

- 向策略视图 (/api/policy-rules/{policyRuleId}) 表达式（ “developerScanExpression” ）添加了新的布尔值字段，以标识快速扫描类型。

修复了版本 2021.6.0 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-21613)。修复了一个问题：scan.cli 版本 2019.8.x 显示无意义的警告消息，以表明性能因使用的 Java 版本而出现下降。
- （Hub-25227、25521）。修复了一个问题：“扫描” 页面上的 “扫描完成” 状态存在误导性。
- (Hub-26108)。修复了以下问题：使用客户证书时，如果部署带有警报的 Black Duck，需要手动干预 nginx 警报配置文件。
- (Hub-26924)。修复了一个问题，现在当 SAML SSO 用户登录失败时会显示用户容易理解的错误消息。
- (Hub-27209)。修复了 VersionBomComputationJob 失败并显示以下错误的问题：“作业执行出错：无法提取 ResultSet；SQL [n/a] ；限制 [cvss2_severity]。”
- (Hub-27681)。修复了使用自定义安全上下文在 Kubernetes 上部署时 BOM 引擎必须由 root 用户启动的问题。
- (Hub-27894)。修复了以下问题：在新的 Black Duck 搜索中将重置设为 0。
- (Hub-28171)。修复了以下问题：一个项目的版权搜索失败。
- (Hub-28305)。修复了日志中出现以下错误的问题：类 com.blackducksoftware.job.integration.domain.impl.JobMaintenanceJob 失败。
- (Hub-28347)。修复了以下问题：代码段调整导致出现重复密钥 SnippetAdjustment 错误。
- (Hub-28351)。修复了保存 BOM 许可证更改时的性能问题。
- (Hub-28469)。修复了以下问题：无法使用 Docker 20.10.x 配置自定义证书。
- (Hub-28726)。修复了以下问题：克隆项目后，Black Duck 会将克隆项目的用户名显示为组件审查者的名称。
- (Hub-28909)。修复了以下问题：锁定用户帐户后，Black Duck UI 中出现了不正确的错误消息。
- (Hub-29071)。修复了批量编辑代码段时的性能问题。
- (Hub-29168)。修复了以下问题：如果映射到项目版本的扫描中没有匹配项，则项目级文件调整不会应用于该项目版本。

Black Duck SCA 2021.4.x

版本 2021.4.1 中的新增功能和更改功能

Black Duck 版本 2021.4.1 是维护版本，不包含新增功能或更改的功能。

修复了版本 2021.4.1 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-28347)。修复了批量代码段调整失败并出现以下错误的问题：“调整失败：服务器遇到错误，请检查您的连接并重试。”

- (Hub-28807)。修复了 Artifactory 插件中出现以下错误的问题： “在 /api/projects/<projectID>/versions/<projectVersionID>/components/<componentID>/versions/<componentVersionID>?offset=0&limit=100 上存在太多参数错误。”
- (Hub-29002)。修复了以下问题：在“代码段确认”窗口中筛选未忽略的代码段时，显示了系统范围的代码段。
- (Hub-29448)。修复了以下问题：LDAP 用户授权失败并出现 IncorrectResultSizeDataAccessException 错误。

版本 2021.4.0 的公告

新容器和系统要求的变更

在 2021.6.0 版本中：

- 将添加一个新容器 blackduck-webui，用于提高 Black Duck 性能、改进缓存和实现未来的可扩展性。
- 快速扫描功能将提供给所有 Black Duck 客户使用。此功能需要一个新的容器（当前名为 blackduck-kb），该容器将管理与 Black Duck KnowledgeBase 的连接，并以较短的时间间隔缓存 KnowledgeBase 结果。

以下是运行所有容器的单个实例所需的最低硬件。请注意，内存要求取决于您要支持的并发快速扫描的数量。

- 7 个 CPU
- 28.5 GB RAM（最低 Redis 配置）；31.5 GB RAM（最佳配置），以便为 Redis 驱动的高速缓存提供更高的可用性。这将支持多达 100 个并发快速扫描。

  30 GB RAM（最低 Redis 配置）；33 GB RAM（最佳配置），以便为 Redis 驱动的高速缓存提供更高的可用性。这将支持超过 150 次快速扫描，但支持的快速扫描的最大数量仍待确定。
- 250 GB 可用磁盘空间，用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

以下是运行带有 Black Duck 二进制分析 的 Black Duck 所需的最低硬件。

- 8 个 CPU
- 32.5 GB RAM（最低 Redis 配置）；35.5 GB RAM（最佳配置），以便为 Redis 驱动的高速缓存提供更高的可用性。这将支持多达 100 个并发快速扫描。

  34 GB RAM（最低 Redis 配置）；37 GB RAM（最佳配置），以便为 Redis 驱动的高速缓存提供更高的可用性。这将支持超过 150 次快速扫描，但支持的快速扫描的最大数量仍待确定。
- 350 GB 可用磁盘空间，用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

注：每个附加的 binaryscanner 容器都需要一个额外的 CPU、2 GB RAM 和 100 GB 可用磁盘空间。

未映射的代码位置的保留期

在 Black Duck 2021.6.0 版本中，未映射的代码位置的默认保留期将从 365 天更改为 30 天。

已弃用的 API

以下端点已被弃用，将在将来的版本中移除：

```
GET /api/scan/{scanId}/bom-entries
```

自 2021 年 4 月 30 日起，将弃用以下端点：

```
GET /api/components/{componentId}/versions/{componentVersionId}/origins/{originId}/
direct-dependencies
```

2021.6.0 版本中的新作业实施

在 Black Duck 版本 2021.6.0 中，作业子系统正在被新的实施取代，这将导致以下作业 Rest API 调用无法运行。

- `GET /jobs/{jobID}`

  此调用按 ID 获取特定作业的作业详细信息。从 Black Duck 2021.6.0 版本开始，此调用将返回“404 Not Found”状态代码。

以下调用自 Black Duck 版本 2020.2.0 起停止使用，将返回“404 Not Found”状态代码，并且在 Black Duck 版本 2021.6.0 中将保持无法使用。

- `PUT /jobs/{jobID}`

  此调用会重新安排作业。

- `DELETE /jobs/{jobID}`

  此调用会终止作业。

该功能将被新的作业 Rest API 实施所取代，该实施将在未来的版本中提供。

日语

2021.2.0 版本的 UI、联机帮助和发行说明已本地化为日语。

版本 2021.4.0 中的新增功能和更改功能

快速扫描 - 受限的客户可用功能

Black Duck快速扫描为开发人员提供了一种方法，以快速确定项目中包含的开源组件版本是否违反了与使用开源组件有关的公司策略。通过使用 Black Duck Detect，快速扫描可以快速返回结果，因为它只使用软件包管理器扫描，并且不与 Black Duck 服务器数据库交互。当您需要快速反馈时，以及不需要在 Black Duck 中保留数据时，请使用快速扫描。

通过使用快速扫描，您可以运行数千次扫描，同时无需部署更多的 Black Duck 实例。它为您提供了可行的结果（比如构建失败），您可以在没有项目版本或无法访问 Black Duck 用户界面的情况下使用这些结果。

注: 在 2021.4.0 版本中，快速扫描是一项受限的客户访问功能。要使用快速扫描，请与 Black Duck 客户管理团队联系以获得帮助。

重复 BOM 检测

Black Duck 添加了重复 BOM 检测，用于确定新的软件包管理器扫描是否与现有 BOM 重复，如果重复，则停止处理扫描并表示扫描已完成。对于生成冗余（相同）数据的高频扫描，Black Duck 的重复 BOM 检测可以显著提高性能。

在 Black Duck 2021.4.0 中，只有当 Black Duck Detect 发现的依赖关系组合与上一个扫描发现的组合相同时，此功能才会影响软件包管理器（依赖关系）扫描。此功能将在未来的版本中扩展。

配置项目经理角色的能力

Black Duck 现在允许系统管理员定义项目经理角色是否可以管理策略违反（覆盖策略违反或移除覆盖）或修复项目的安全漏洞。

默认情况下，具有“项目经理”角色的用户可以管理策略违反并修复安全漏洞：升级到版本 2021.4.0 的用户将不会看到项目经理角色发生任何更改。

多许可证编辑增强

在编辑 KnowledgeBase 或自定义组件版本的许可证时，Black Duck 现在使您能够在 root 级别或与原始许可证相同的级别为组件轻松创建新的或编辑现有的多许可证方案。

深度许可证数据增强

Black Duck 现在可以添加文件级深度许可证或移除手动添加的许可证。

报告增强

- 对组件项目版本报告 (component_date_time.csv) 进行了以下增强：
  - 新列“组件来源 ID”已添加到报告的末尾。此列提供了以前只能使用 API 获取的组件来源 ID 值。
  - 用户名、日期和时间已添加到“备注”列中列出的每个备注中。
- 在升级指导项目版本报告 (project_version_upgrade_guidance_date_time.csv) 的末尾添加了一个新列“知识库超时”。它指示在获取组件版本/来源的升级指导数据时是否出现 Black Duck KnowledgeBase 超时错误。

策略管理增强

- 策略规则可用的项目和组件条件已按类别重新整理，以便更容易查找和选择条件。此外，项目和组件的自定义字段已按自定义字段的类型进行分隔。
- 新的许可证条件“已声明或深度许可证的许可证到期日期比较”允许您将许可证到期日期与项目版本的发布日期进行比较。

漏洞影响增强

现在可以使用策略规则的新漏洞条件“可从来源访问”，使您能够为已被确定为可访问的漏洞创建策略规则。使用此条件，以不同（更高）的优先级排列这些漏洞的优先级。

对 LDAP 或 SAML 组同步的更改

为了减少身份验证错误，Black Duck 修改了 LDAP 或 SAML 组同步。现在，如果在为 Black Duck 配置 LDAP 或 SAML 时启用了组同步，则 LDAP 或 SAML 服务器和 Black Duck 服务器上的组名称必须相同。如果您在 Black Duck 中更改组的名称，则还必须更改 LDAP 或 SAML 服务器上的组名称以匹配新名称（反之亦然）。如果名称不相同，则组可能不同步，该组的用户权限将丢失。

容器增强

向 Binaryscanner 容器添加了运行状况检查。

对“来源”选项卡的增强

已将新的筛选器“代码视图可用”添加到项目版本的来源选项卡中。

组件和项目搜索增强

组件和项目搜索的“查找”页面现在提供了对搜索结果进行排序的功能。

保存的搜索增强

保存的搜索支持搜索结果排序，使您可以在“仪表板”页面上按感兴趣的顺序查看结果。

项目名称页面的性能改进

要提高性能，现在必须选择“策略违反”图标 (⦸) 或“覆盖”图标 (ⓘ)，以在项目名称页面的概述选项卡上查看策略违反信息。

克隆增强

对克隆项目版本进行了以下增强：

- 默认克隆选项已更改。现在，所有克隆选项都在创建项目时启用。
- 添加了一个新选项版本设置，用于克隆这些值：
  - 许可证
  - 备注
  - 昵称
  - 发布日期
  - 阶段
  - 分发
- 当您从项目名称页面选择克隆时，将出现一个新的“克隆版本”对话框。如果启用了版本设置克隆选项，则对话框中只会显示新版本名称。
- 为了消除混淆，已从“创建新版本”对话框中移除了要克隆的版本字段。

许可证冲突增强

手动编辑 BOM 时（包括使用许可证冲突或组件选项卡更改组件或项目版本许可证的使用）现在将触发重新计算许可证冲突。

“系统信息”页面的增强

“系统信息”页面上的使用类别已得到增强。

- 在使用：项目部分，“按项目列出的扫描”部分现在列出了“按项目列出的前 10 个扫描”。
- 在使用：快速扫描完成部分，“按用户列出的快速扫描”现在列出了“按用户列出的前 10 个快速扫描”。
- 使用：扫描完成部分已重新格式化为表格，并包括用于重复 BOM 检测的“相同的软件包管理器”行。还添加了两个新表：“代码位置摘要信息”和“重复 BOM 信息”。

这些页面显示六个月的数据或系统拥有数据的月数所对应的数据，以值较小的为准。

新作业 CollectScanStatsJob 可收集“系统信息”页面上使用：扫描完成部分显示的扫描统计信息。

移除安装指南

已从文档集中移除使用 Kubernetes 安装 Black Duck 和使用 OpenShift 安装 Black Duck 指南。这些文档仅包含最新文档的链接。这些链接已添加到每个 PDF 中的 Black Duck 文档页面和联机帮助的主页。

项目名称页面的增强

项目名称页面已重新组织和增强，现在包括每个项目版本的上次扫描日期。

“仪表板” 页面的增强

在 “仪表板” 页面上，“策略违反饼图” 中的 “无” 的 “策略违反” 值以前会返回 100%（无违反）或 0%（一些违反），现在反映了违反的实际百分比。

支持的浏览器版本

- Safari 版本 14.0.3（15610.4.3.1.7，15610）
- Chrome 版本 90.0.4430.72（正式版本）(x86_64)
- Firefox 版本 88.0（64 位）
- Microsoft Edge 版本 90.0.818.41（正式版本）（64 位）

容器版本

- 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

日语

2021.2.0 版本的 UI、联机帮助和发行说明已本地化为日语。

API 增强

- 添加了通过 /api-doc/postman-collection-public.json 在 API 文档中生成 Postman 集合的功能。用户可以将 postman-collection-public.json 文件作为 Postman 集合导入到 Postman 中。
- 添加了通过 /api-doc/openapi3-public.json 为面向客户的端点生成 OpenAPI 规格 (OAS) 的功能。
- 添加了通过使用 /api/projects?filter=owner 按项目所有者筛选项目的功能，该功能使用用户的 URL 搜索用户拥有的项目，例如 /api/projects?filter=owner:https://<bd_server>/api/users/。
- 已将许可证所有权信息作为新的所有权字段添加到 /projects/{projectId}/versions/{projectVersionId}/components 端点。
- 添加了用于读取和更改以下应用程序设置的 API：

  - 读取分析设置
    `GET /api/settings/analysis`
  - 更新分析设置
    `PUT /api/settings/analysis`
  - 读取品牌设置
    `GET /api/settings/branding`
  - 更新品牌设置
    `PUT /api/settings/branding`
  - 读取许可证审查设置
    `GET /api/settings/license-review`
  - 更新许可证审查设置
    `PUT /api/settings/license-review`
  - 读取角色设置
    `GET /api/settings/role`
  - 更新角色设置
    `PUT /api/settings/role`
- 添加 /api/component-migrations 和 /api/component-migrations/{componentOrVersionId} 端点，以便根据特定日期或特定组件从 KnowledgeBase 获取组件迁移数据。
- 使 /license-dashboard API 公开，允许用户查看使用中的许可证。
- 解决了一个问题：当漏洞有 100 个以上的引用时，api/vulnerabilities/{vulnerabilityId} 端点返回标头溢出错误。现在，当响应标头中返回 25 个或更多链接标头时，端点将发出警告，并在响应正文中包括元链接。
- 从“活动/日志”端点移除了“触发器类型”筛选器，因为它仅用于“用户”类型。

修复了版本 2021.4.0 中的问题

在此发布中修复了客户报告的以下问题：

- （Hub-24015、26281）。修复了在 Black Duck 用户界面中出现的间歇性权限被拒错误。
- (HUB-25116)。修复了以下问题：对于以 UCS-2 编码的文件，“代码段视图”对话框中出现红点，导致文本不可读。
- (HUB-25549)。修复了 /api/uploads 的一个问题：codeLocationName 包含日语字符时，创建的代码位置未映射到项目版本。
- (HUB-25550)。已将 BOM 更新信息添加到项目版本的活动/日志中。
- （HUB-25605、27618）。修复了使用 /api/tokens/authenticate 通过 API 令牌进行身份验证时的问题：在该令牌过期后，HTTP 客户端被重定向到 SAML 提供程序页面，或者在生成 PDF 报告时发生错误。
- (Hub-25993)。修复了重复记录导致作业运行器日志中出现以下错误消息的问题：“冲突对象已存在。”
- (Hub-26481)。修复了以下问题：保存新的修复状态后页面会完全刷新。
- (HUB-26588)。修复了以下问题：对 android-studio-ide-201.7199119-windows.exe 运行二进制扫描失败。
- (Hub-26695)。修复了以下问题：一天中某些时候的扫描时间明显延长。

- (Hub-26897)。修复了一个问题，以便为组件名称页面上未列出的无效版本显示“404 Not Found”错误代码。
- (Hub-26911)。修复了以下问题：选择替代代码段匹配会错误地将组件识别为已使用加密。
- (Hub-27159)。修复了使用“去年的贡献者”、“去年的提交”或“新版本计数”组件条件的策略规则存在的问题。尽管这些条件被定义为在值等于 0 时触发违反，但当值大于 0 或组件没有提交历史记录时，也会触发策略违反。

  注：通过此修复，新的扫描或重新扫描可能会移除以前触发的一些策略违反。
- (Hub-27167)。修复了以下问题：分配到具有全局项目查看者角色的非活动组的活动用户可以查看仪表板中的所有项目。
- (Hub-27175)。修复了以下问题：因为组件名称页面上的使用计数值基于组件来源的数量，而不是基于组件版本，所以该计数不准确。
- (Hub-27282)。修复了以下问题：BOM 中的策略违规弹出窗口偶尔卡在打开状态，并且除非刷新页面，否则无法关闭该窗口。
- （Hub-27284、27660）。修复了以下问题：某些动态链接组件的匹配类型为过渡依赖关系，但在项目版本 BOM 的来源列中缺少匹配信息。
- (Hub-27287)。修复了一个问题，以便项目名称页面上的概览选项卡上显示的风险计数使用组件版本值（与 BOM 页面一样），而不是按组件来源计算。
- (Hub-27293)。修复了以下问题：重新扫描项目时，标记为“已审查”的组件被标记为“未审查”。
- (Hub-27306)。修复了以下问题：在“通知报告”中按区分大小写的顺序列出组件。
- (Hub-27308)。修复了以下问题：更改组件版本的许可证后，Black Duck KB 组件名称页面未正确显示漏洞数量。
- (Hub-27326)。修复了以下问题：使用项目的设置选项卡删除应用程序 ID 时，实际上并未删除应用程序 ID。
- (Hub-27613)。修复了以下问题：在来源选项卡中无法浏览二进制文件的源文件。
- (Hub-27961)。修复了“仪表板”页面上图形的图例，使其看起来不可点击。
- (Hub-27982)。修复了以下问题：二进制扫描仅识别 MSI 存档中的第一个和最后一个文件。
- (Hub-27985)。修复了以下问题：在 Black Duck 构建 BOM 时会出现消息，当向下滚动 BOM 页面时，该消息会消失。
- (Hub-28094)。修复了以下问题：/api/usergroups 端点未在搜索词中正确使用“_”或“%”。
- (Hub-28165)。修复了在 BOM 页面上编辑许可证的问题：选择“取消/关闭”仍会应用更改。
- (Hub-28208)。修复了以下问题：“注册”页面上显示的代码库大小不正确。
- (Hub-28226)。修复了一个问题，现在，在取消映射或删除引入组件的代码位置时，违反一项或多项策略的组件会生成“策略已清除”通知。
- (Hub-28259)。修复了取消审查/取消忽略 SQL 查询分析存在的问题。
- (Hub-28292)。修复了以下问题：HELM T 恤尺寸 .yml 文件未扩展 BOM 引擎容器。
- (Hub-28370)。修复了以下问题：使用 BOM 比较视图时未显示严重漏洞。
- (Hub-28375)。修复了一个问题，以便 CVE 或 BDBA 记录的受影响的项目选项卡不再显示已被忽略的组件的漏洞。
- (Hub-28383)。修复了以下问题：如果筛选了项目名称页面，导致页面上只显示一个版本，则无法删除该版本。

- (Hub-28416)。修复了以下问题：无法修改一组许可证的 AND 或 OR 运算符。
- (Hub-28458)。修复了以下问题：SnippetScanAutoBom 作业显示“作业执行时出错：重复密钥”错误消息。
- (Hub-28562)。修复了二进制扫描的问题：扫描无法完成后期工作并出现以下错误消息：“路径不是 null 的父级。”
- (Hub-28580)。修复了尝试访问我的访问令牌页面时出现的问题，此问题导致出现以下错误：“应用程序遇到未知错误。”
- (Hub-28639)。修复了以下问题：如果项目名称同时包含英文和中文字符，已下载报告文件的后缀扩展名为 .json，而不是 .zip。
- (Hub-28681)。修复了以下问题：当匹配类型为直接或过渡依赖关系时，在来源选项卡上会显示使用情况。
- (Hub-28765)。修复了以下问题：BOM 页面会显示已确认和已忽略的代码段。
- (Hub-28773)。修复了一个问题，以便从 hub-webserver.env 文件中的 TLS_PROTOCOLS 选项中移除 TLSv1.1。

Black Duck SCA 2021.2.x

版本 2021.2.1 中的新增功能和更改功能

Black Duck 版本 2021.2.1 是维护版本，不包含新增功能或更改的功能。

修复了版本 2021.2.1 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-23928)。修复了以下问题：重新扫描后会更改已确认的代码段匹配。
- (Hub-26898)。修复了以下问题：似乎已完成扫描，但 Black Duck Detect 会超时，因为它无法从 Black Duck 获得 bom_complete 通知。
- (Hub-27688)。修复了以下问题：匹配文件的 API 调用未返回任何过渡和直接依赖关系匹配的信息。
- (Hub-28410)。修复了无法在 Kubernetes 上启动 RabbitMQ 容器的问题，通过引入持久性卷来解决该问题。
- （Hub-28208、28386）。修复了以下问题：“产品注册”页面上显示错误的代码库大小。
- (Hub-28278)。修复了以下问题：RabbitMQ 容器缺少持久卷导致 BOM 引擎中的日志记录过多且扫描失败。
- (Hub-28292)。修复了缩放 BOM 引擎容器的问题。

版本 2021.2.0 的公告

Azure 客户通知

Black Duck 版本 2021.2.0 在发布时存在一个已知问题，该问题影响在 Azure Kubernetes Services (AKS) 上部署并将 Azure Database for PostgreSQL 用作外部数据库的客户。请注意，这是针对 Azure 平台上的 Black Duck 客户推荐的标准配置。目前，不建议在具有外部数据库的 Azure 平台上运行的客户升级到 2021.2.0。这样做将使系统无法运行，并迫使您将安装恢复到先前的状态。

我们预计这一问题将在未来的 Black Duck 版本中得到解决，并将在版本详细信息已知时发布公告。

如果您在 AKS 上运行并使用内部 PostgreSQL 数据库，则不会出现问题，系统将按预期工作。但是，这将是在 AKS 平台上的非典型安装。

如果您有任何疑虑和疑问，请联系 Black Duck 支持部门寻求帮助。

对外部数据库弃用 PostgreSQL 版本 9.6

Black Duck 从 Black Duck 2021.6.0 版本开始，不再支持将 PostgreSQL 版本 9.6 用于外部数据库。

从 Black Duck 2021.6.0 版本开始，Black Duck 只支持将 PostgreSQL 版本 11.x 用于外部数据库。

不再支持 Internet Explorer 11

Black Duck 已终止对 Internet Explorer 11 的支持。

已弃用的页面

“扫描 > 组件”页面从 2021.2.0 版本开始弃用，并将在将来的版本中移除。

日语

2020.12.0 版本的 UI、联机帮助和发行说明已本地化为日语。

版本 2021.2.0 中的新增功能和更改功能

新的自定义漏洞仪表板

为了便于您轻松查看对您至关重要的漏洞，在 2021.2.0 中，“安全”仪表板已根据您保存的漏洞搜索替换为自定义漏洞仪表板。 Black Duck 现在允许您使用各种属性搜索您的项目和/或 Black Duck KnowledgeBase 中使用的漏洞，保存搜索，然后使用“仪表板”页面从这些保存的搜索中查看仪表板。

对于每个漏洞，自定义漏洞仪表板显示以下信息：

- BDSA 或 NVD 漏洞 ID。选择漏洞 ID 以显示有关漏洞的更多信息，比如其他分数值。
- 受此漏洞影响的项目版本数，带有可查看漏洞的受影响的项目选项卡的链接，该选项卡列出了受此漏洞影响的项目版本。
- 总体风险评分。
- 解决方案、解决方法或漏洞利用是否可用。
- 首次检测、发布和最后修改漏洞的日期。
- 此安全漏洞的常见弱点枚举 (CWE) 编号。

漏洞搜索增强

通过可用于搜索漏洞的属性以及搜索结果中显示的信息，可以增强漏洞搜索功能。您可以选择是搜索项目中的漏洞还是 Black Duck KnowledgeBase 中的漏洞。

搜索漏洞时，可以使用以下属性：

- 影响项目
- 默认修复
- 可到达
- 漏洞利用
- 首次检测到

- 修复状态
- 解决方案
- 基本分数
- 可利用性分数
- 影响分数
- 总体得分
- 发布年份
- 严重性
- 来源（BDSA 或 NVD）
- 时间分数
- 解决方法

现在可以保存这些漏洞搜索结果并在“仪表板”页面中查看，如上所述。

能够管理项目的许可证冲突

为了降低许可证侵权的风险，您需要了解 BOM 中的组件拥有的许可证的条款与项目声明的许可证不兼容的情况。 Black Duck 现在可以识别这些许可条款冲突，并将它们显示在位于法律选项卡上的新的许可证冲突选项卡上。

您还可以设置在组件的许可证与项目版本的许可证冲突时触发的策略规则。

请注意，Black Duck 仅确定许可证风险较高的组件版本的许可证冲突。对于 Black Duck 许可证风险模型，“高风险”意味着此系列中的许可证在该业务场景（分发类型和组件用法组合）下往往存在许可证冲突，从而导致许可证不兼容。中或低风险意味着，如果业务场景发生变化（或定义不正确）或由于其他非许可证冲突因素，它可能会存在风险。

依赖关系

在 Black Duck Detect 扫描中发现直接或过渡依赖关系时，Black Duck 现在会在项目版本的安全选项卡中列出每种依赖关系类型的匹配数。

对于过渡依赖关系，依赖关系树显示引入此依赖关系的组件、按严重性级别列出的漏洞以及使用该依赖关系路径引入组件的次数的匹配计数。

报告数据库增强

已将忽略的组件的新表 (component_ignored) 添加到报告数据库中。它包含以下列：

- id。ID
- project_version_id。项目版本 ID。
- component_id。组件 ID。
- component_version_id。组件版本 ID。
- component_name。组件名称。
- component_version_name。组件版本名称。
- version_origin_id。版本来源 ID。
- origin_id。来源 ID。
- origin_name。来源名称。

- ignored。布尔值，指示是否忽略组件。
- policy_approval_status。策略审批状态。
- review_status。查看组件的状态。
- reviewed_by。审查组件的用户。
- reviewed_on。审查组件的时间。
- security_critical_count。严重安全漏洞的数量。
- security_high_count。高风险安全漏洞的数量。
- security_medium_count。中等风险安全漏洞的数量。
- security_low_count。低风险安全漏洞的数量。
- security_ok_count。无风险安全漏洞的数量。
- license_high_count。高许可证风险的数量。
- license_medium_count。中等许可证风险的数量。
- license_low_count。低许可证风险的数量。
- license_ok_count。无许可证风险的数量。
- operational_high_count。高运维风险的数量。
- operational_medium_count。中等运维风险的数量。
- operational_low_count。低运维风险的数量。
- operational_ok_count。无运维风险的数量。

已将用户信息的新表 (user) 添加到报告数据库中。它包含以下列。

- id。ID。
- first_name。用户的名字。
- last_name。用户的姓氏。
- username。Black Duck 中用户的用户名。
- email。用户的电子邮件地址。
- active。表示此用户是否处于活动状态的布尔值。
- last_login。用户上次登录到 Black Duck 的时间。

许可证编辑增强

在 BOM 中编辑许可证时进行了以下增强。

- 在编辑组件的许可证时，Black Duck 现在使您能够在 root 级别或与原始许可证相同的级别为 BOM 中的组件轻松创建新的或编辑现有的多许可证方案。
- 如果为组件选择了不同的许可证，您现在可以将许可证恢复为 Black Duck KnowledgeBase 中定义的原始许可证。
- 组件名称版本“组件许可证”对话框中的一个新选项使您可以轻松地看到存在编辑模式。

报告增强

source_date_time.csv 项目版本报告的末尾添加了一个新列“存档上下文和路径”。此列将现有“路径”和“存档内容”列中显示的信息串联在一起，以提供每个组件的完整路径。

通知文件报告

通知文件报告已得到改进，版权数据不再包含单个组件来源的重复信息。

二进制扫描增强

现在，二进制扫描除了返回完全匹配之外，还返回部分匹配。

深度许可证数据增强

在审查文件中深度许可证数据的证据时，Black Duck 现在会突出显示触发许可证文本匹配的许可证文本。

BOM 引擎

为了缩短 Black Duck UI 响应时间，现在将由 BOM 引擎执行许可证更新。此过程可在“BOM 处理状态”对话框中显示为“许可证更新”或“许可条款履行更新”事件，可从 BOM 访问该对话框。

Black Duck 教程

为了方便查看 Black Duck 培训，您现在可以选择 Black Duck 教程（从“帮助”菜单 ()（位于 Black Duck UI 中）选择）。

修改密码配置

具有“系统管理员”角色的用户现在可以为本地 Black Duck 帐户设置密码要求。具有“超级用户”角色的用户无法再配置密码要求。

策略规则增强

策略管理现在提供了基于项目版本自定义字段创建策略规则的功能，这些字段包括布尔值、日期、下拉列表、多选、单选和文本字段类型。

的托管位置 Black Duck Detect

Black Duck 外部连接受限的客户现在可以定义 Black Duck Detect 的内部托管位置。使用此信息，这些用户可以利用 Code Sight 在其开发人员库中进行部署，以运行按需软件组合分析 (SCA) 扫描。

保存的搜索仪表板增强

对于“仪表板”页面上显示的每个已保存搜索，Black Duck 现在会列出上次更新搜索的日期和时间。弹出窗口将显示保存的搜索过滤器以及一个链接，使您可以打开“查找”页面以编辑和保存修订后的已保存搜索。

代码段分类增强

已将图标添加到来源选项卡，以便更容易区分未确认 ()、已确认 () 和已忽略 () 代码段。

支持的浏览器版本

- Safari 版本 14.0.3（156104.3.1.6、15610）
- Chrome 版本 88.0.4324.150（正式版本）(x86_64)
- Firefox 版本 85.0.2（64 位）
- Microsoft Edge 版本 88.0.705.63（正式版本）（64 位）

容器版本

- 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

支持的 Docker 版本

Black Duck 安装支持 Docker 版本 18.09.x、19.03.x 和 20.10.x（CE 或 EE）。

Docker webapp-volume

Docker webapp-volume 不再用于编排。（可选）用户可以备份和修整 Docker webapp-volume；其他情况下不需要执行任何操作。

Ubuntu 操作系统

适合在 Docker 环境中安装 Black Duck 的首选 Ubuntu 操作系统现在为版本 18.04.x。

日语

2020.12.0 版本的 UI、联机帮助和发行说明已本地化为日语。

API 增强

- API 文档现在只能在 https://<Black Duck server URL>/api-doc/public.html 上获得。
- 增加了按创建日期过滤代码位置 (/api/codelocations) 的功能。
- 修复了用于下载 SAML 身份提供程序元数据 XML 文件 (api/sso/idp-metadata endpoint) 的 API，该 API 在以前的版本中运行出错。
- 修复指导端点 (GET /api/components/{componentId}/versions/{componentVersionId}/remediating) 不再返回“410 GONE”响应。您必须切换到升级指导端点 (GET /api/components/{componentId}/versions/{componentVersionId}/upgrade-guidance)，该端点与已移除的修复指导端点不兼容。
- 添加了报告依赖关系路径端点以显示组件的依赖关系路径：

  /api/project/{projectId}/version/{projectVersionId}/origin/{originId}/dependency-paths

- 添加了 Black Duck Detect URI 端点，仅用于设置或更新读取“系统设置”页面上的 Black Duck Detect URI：

  /external-config/detect-uri

修复了版本 2021.2.0 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-22103)。修复了以下问题：Black Duck 服务器在更新许可证状态时没有及时响应。
- (Hub-22623)。修复了企业客户在 UI 中加载“摘要仪表板”时仪表板经常超时的问题。
- (Hub-24332)。修复了扫描相同代码位置导致重复通知的问题。
- (Hub-25374)。修复了数据库 azure_maintenance 的权限错误。
- (Hub-25580)。修复了 BOM 中显示的组件在第 9 页之后排序错误的问题。
- (Hub-25666)。修复了端点 /usergroups/<group #>/role 的分页问题。
- (Hub-26030)。修复了在执行操作后未按项目名称为仪表板保留排序选项的问题。
- (Hub-26324)。修复了上传扫描时出现以下错误“java.lang.IllegalStateException: [file:/C:/src/External/PackageManager/ProjectTemplates/com.unity.template.universal-10.1.0.tgz] 的父级不存在”的问题。
- (Hub-26343)。修复了无法注册 Black Duck 的问题，因为注册容器的堆空间不足。
- (Hub-26493)。修复了当用户移除自己项目成员身份时出现的混淆错误消息。
- (Hub-26501)。修复了无法在“编辑组件”对话框中选择 cordova-plugin-inappbrowser 组件的问题。
- (Hub-26536)。修复了关注的项目在页面标题中显示“未关注”图标（  ）的问题。
- (Hub-26540)。修复了以下问题：除非重新启动 Black Duck，否则 SAML 的初始配置不会生效。
- (Hub-26615)。修复了在项目 A 中具有“项目经理”角色和项目 B 中具有“项目经理”和“项目代码扫描者”角色的用户可以将扫描上传到项目 A 的问题。
- (Hub-26616)。修复了尝试忽略代码段失败并显示以下错误消息的问题：“无法更新现有代码段调整，因为不支持更改使用方、生产者、调整类型、起始行、结束行。”
- （Hub-26712、26962）。修复了在确认代码段匹配后，来源选项卡树视图中显示的代码段图标未清除的问题。
- (Hub-26726)。修复了创建策略规则时不能为自定义字段使用“不在内部”选项的问题。
- (Hub-26807)。修复了在尝试获取 BOM 组件版本的自定义字段时收到 HTML 状态代码 404 的问题。
- (Hub-26815)。修复了保存 SAML 集成设置导致页面重新加载并切换“身份提供程序元数据”设置的问题。
- (Hub-26904)。修复了设置选项卡上项目版本活动部分显示的匹配计数值与扫描名称页面上显示的值不同的问题。
- (Hub-26930)。修复了未触发组件通知的问题。
- (Hub-27002)。修复了创建克隆项目时发送错误通知的问题。
- (Hub-27049)。修复了以下问题：在没有为用户分配“许可证经理”角色的情况下，无法在 Black Duck UI 中看到项目版本报告的“许可条款”类别。
- (Hub-27208)。修复了以下问题：在配置 SAML 时 Black Duck Alert 无法加载 blackduck-nginx。
- (Hub-27227)。修复了代码段匹配需要很长时间才能完成的问题。

- (Hub-27264)。修复了审查组件会将其使用方式重置为默认值的问题。
- (Hub-27681)。修复了使用自定义安全上下文在 Kubernetes 上部署时 BOM 引擎必须由 root 用户启动的问题。

Black Duck SCA 2020.12.x

版本 2020.12.0 的公告

新容器和系统要求的变更

还有两个附加容器：2020.12.0 版本的 BOM 引擎和 RabbitMQ（现在是必需的容器）。

运行所有容器的单个实例的最低系统要求是：

- 6 个 CPU
- 26 GB RAM（最低 Redis 配置）；29 GB RAM（最佳配置），以便为 Redis 驱动的高速缓存提供更高的可用性
- 250 GB 可用磁盘空间，用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

运行带有 Black Duck 二进制分析 的 Black Duck 所需的最低硬件包括：

- 7 个 CPU
- 30 GB RAM（最低 Redis 配置）；33 GB RAM（最佳配置），以便为 Redis 驱动的高速缓存提供更高的可用性
- 350 GB 可用磁盘空间，用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

注：每个附加的 binaryscanner 容器都需要一个额外的 CPU、2 GB RAM 和 100 GB 可用磁盘空间。

终止对 Internet Explorer 11 的支持

对 Internet Explorer 11 的支持已弃用，Black Duck 将从 Black Duck 2021.2.0 版本开始终止对 Internet Explorer 11 的支持。

日语

2020.10.0 版本的 UI、联机帮助和发行说明已本地化为日语。

版本 2020.12.0 中的新增功能和更改功能

新容器和系统要求的变更

还有两个附加容器：2020.12.0 版本的 BOM 引擎和 RabbitMQ（现在是必需的容器）。

运行所有容器的单个实例的最低系统要求是：

- 6 个 CPU
- 26 GB RAM（最低 Redis 配置）；29 GB RAM（最佳配置），以便为 Redis 驱动的高速缓存提供更高的可用性
- 250 GB 可用磁盘空间，用于数据库和其他 Black Duck 容器

- 数据库备份的相应空间

运行带有 Black Duck 二进制分析 的 Black Duck 所需的最低硬件包括：

- 7 个 CPU
- 30 GB RAM（最低 Redis 配置）；33 GB RAM（最佳配置），以便为 Redis 驱动的高速缓存提供更高的可用性
- 350 GB 可用磁盘空间，用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

注：每个附加的 binaryscanner 容器都需要一个额外的 CPU、2 GB RAM 和 100 GB 可用磁盘空间。

密码配置

具有“超级用户”角色的用户现在可以为本地 Black Duck 帐户设置密码要求。如果启用，Black Duck 将确保新密码符合您的要求，并拒绝被认为较弱的密码，比如 "password"、"blackduck" 或用户的用户名或电子邮件地址。

超级用户可以：

- 定义最小密码长度。
- 定义密码的最小字符类型数。可能的字符类型包括小写字母、大写字母、数字或特殊字符。
- 选择是否在当前用户登录 Black Duck 时对其强制执行密码要求。

默认情况下，将启用密码要求并具有以下设置：

- 密码的最小长度为八个字符。
- 只需要一种字符类型。
- 登录 Black Duck 时，不对当前用户强制执行密码要求。

许可证增强

为了成功管理许可证风险，Black Duck 现在允许您为 BOM 中的组件创建新的或编辑现有的多许可证方案。

漏洞影响分析增强

- 已添加新的项目版本报告 vulnerability_matches_date_time.csv。列出漏洞可能接触的每个组件的组件、漏洞数据和漏洞影响分析数据。此报告包含以下列：
  - 组件名称
  - 组件 id
  - 正在使用
  - 组件版本名称
  - 版本 id
  - 渠道版本来源
  - 来源 id
  - 来源名称 id
  - 漏洞 id
  - 漏洞来源
  - CVSS 版本

  - 安全风险
  - 基本分数
  - 总体得分
  - 可用的解决方案
  - 可用的解决方法
  - 可用的漏洞利用
  - 调用的函数
  - 合格名称
  - 行号
- 报告数据库中添加了一个新表，即漏洞方法匹配 (vulnerability_method_matches)。它包含以下列：
  - id。ID。
  - project_version_id。出现可访问漏洞的项目版本的 UUID。
  - vuln_source。漏洞的来源。对于漏洞影响分析，值为 BDSA。
  - vuln_id。漏洞 ID，比如 BDSA-2020-1234。
  - qualified_name。调用函数的类的名称。
  - called_function。代码中容易受到攻击的函数调用的名称，该函数调用使得漏洞可访问。
  - line_number。代码中调用了容易受到攻击的函数的行号。
- 漏洞报告（漏洞修复报告、漏洞状态报告和漏洞更新报告）现在在报告的末尾添加了一个新列“可访问”，以表示安全漏洞是可访问 (true) 还是不可访问 (false)。

BOM 计算信息

Black Duck 现在提供了有关项目版本 BOM 计算状态的详细信息。

Black Duck UI 中项目版本标题中的新状态指示符（取代“组件”指示符）提供 BOM 的当前状态，并通知您 BOM 事件的处理状态。有关更多信息，新的“BOM 处理状态”对话框将列出待定、正在处理或已失败的事件。

Black Duck 还提供配置 BOM 事件清理作业 (VersionBomEventCleanupJob) 的频率的功能，该作业可清除那些由于处理错误或拓扑更改而可能卡滞的 BOM 事件。

策略增强

- 策略管理现在提供了基于以下自定义字段创建策略规则的功能：
  - 布尔值、日期、下拉列表、多选、单选和文本字段类型的组件自定义字段。
  - 布尔值、日期、下拉列表、多选、单选和文本字段类型的组件版本自定义字段。
- 现在，在为以下条件创建策略规则时，您可以区分已声明的许可证数据和深度（嵌入式）许可证数据：
  - 许可证
  - 许可证到期日期
  - 许可证系列

  注:
  使用这些许可证条件的任何现有策略规则现在仅适用于已声明的许可证。您必须为这些许可证条件的深度（嵌入式）许可证创建单独的策略规则。

报告增强

以前仅在全局或项目级别提供的漏洞报告（漏洞修复报告、漏洞状态报告和漏洞更新报告）现在可用于项目版本。

配置代码段文件大小

现在，您可以修改为代码段扫描的默认最大文件大小，并选择 1MB 到 16MB 之间的值。

配置未映射代码位置的清除

Black Duck 每 365 天清除一次未映射的代码位置数据。您可以禁用此功能，以便不清除未映射的代码位置数据，或者，如果您定期扫描并希望经常丢弃数据，则将保留期设置为较低的天数。

访问令牌

现在，用户访问令牌范围的选项为 “读取” 或 “读取和写入” 。

支持的浏览器版本

- Safari 版本 14.0.1 (14610.2.11.51.10)
- Chrome 版本 87.0.4280.88（正式版本）(x86_64)
- Firefox 83.0（64 位）
- Internet Explorer 11 11.630.19041.0

  请注意，对 Internet Explorer 11 的支持已弃用，Black Duck 将从 Black Duck 2021.2.0 版本开始停止对 Internet Explorer 11 的支持。
- Microsoft Edge 87.0.664.60（正式版本）（64 位）

容器版本

- 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

日语

2020.10.0 版本的 UI、联机帮助和发行说明已本地化为日语。

API 增强

- 增加了按 createdAt 字段对项目 (api/projects) 进行排序的功能。
- 增加了过滤在某个日期之前/之后创建的项目的 api/projects 端点的功能。
- 添加了用于显示漏洞匹配的 API，作为漏洞影响分析功能的一部分。

  GET /api/projects/{projectId}/versions/{projectVersionId}/vulnerabilities/{vulnerabilityId}/vulnerability-matches
- 添加了以下 BOM 端点：
  - 获取 BOM 状态摘要：

    GET /api/projects/{projectId}/versions/{projectVersionId}/bom-status
  - 列举 BOM 的事件：

    GET /api/projects/{projectId}/versions/{projectVersionId}/bom-events
  - 删除失败的 BOM 事件：

    DELETE /api/projects/{projectId}/versions/{projectVersionId}/bom-events/{bomEventId}
  - 从 BOM 中删除所有失败的事件：

    DELETE /api/projects/{projectId}/versions/{projectVersionId}/bom-events
- 新密码设置端点：
  - 获取密码设置：

    GET /api/password/security/settings
  - 获取系统密码设置：

    GET /api/password/management/settings
  - 更新系统密码设置：

    PUT /api/password/management/settings
  - 验证密码：

    POST /api/password/security/validate
- /api/catalog-risk-profile-dashboard API 现在返回 “HTTP 404 (Not Found)” 。

修复了版本 2020.12.0 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-24839)。修复了无法从 “添加/编辑组件” 对话框中选择某些组件原始 ID 的问题。
- (Hub-24911)。修复了失败的 KBUpdateJob 跳过组件更新的问题。
- (Hub-25230)。修复了用户尝试打开或编辑许可证文本时未显示许可证文本窗口的问题。
- (Hub-25452)。修复了一个问题，因此在来源选项卡中查看许可证搜索结果页面时，如果选择了许可证类型，则会自动添加发现类型过滤器。
- (Hub-25489)。修复了更改子文件夹时来源选项卡中的过滤器被重置的问题。

- (Hub-25603)。修复了一个问题，因此在选择替代路径时，来源选项卡上“代码段视图”对话框中的匹配文件路径字段中显示的路径会刷新。
- (Hub-25681)。修复了 Protex BOM 工具无法导入通用/未指定组件版本的许可证的问题。
- (Hub-25715)。修复了除非使用鼠标，否则无法修改“自定义字段管理”页面中的“活动”状态的问题。
- (Hub-25739)。修复了无法查看 BOM 组件的所有注释的问题。
- (Hub-25874)。修复了 bom_component_custom_fields_date_time.csv 报告列出的数据与 components_date_time.csv 报告不同（即使数据位于同一列名称中）的问题。
- (Hub-26442)。修复了项目负责人无法在项目版本内删除扫描的问题。
- (Hub-26496)。修复了尽管在更改组件用法时许可证风险已发生变化，但仍触发了许可证风险的策略违反的问题。

Black Duck SCA 2020.10.x

版本 2020.10.1 中的新增功能和更改功能

容器版本

- 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

修复了版本 2020.10.1 中的问题

在此发布中修复了客户报告的以下问题：

- (Hub-25489)。修复了在来源选项卡中选择的过滤器在选择其他文件夹时被重置的问题。
- (Hub-25515)。修复了主机实例运行 TLS 1.3 时特征扫描程序上传失败并显示以下错误消息的问题：“错误：无法保护与主机的连接”。
- (Hub-25791)。修复了从 2020.4.2 版升级到 2020.6.1/2020.6.2 版后扫描时间显著增加的问题。
- (Hub-26027)。修复了 Black Duck 显示以下错误消息的问题：“错误：应用程序遇到未知错误。（错误请求）error.{core.rest.common_error”（尝试上传 Black Duck Detect 扫描时）。

- (Hub-26085)。修复了二进制扫描添加第二个空扫描的问题。

版本 2020.10.0 的公告

新容器和系统要求的变更已推迟到 2020.12.0 版本

Black Duck 此前曾宣布将增加两个容器：2020.10.0 版本的 BOM 引擎和 RabbitMQ（现在是必需的容器）。这一要求已推迟到 2020.12.0 版本。

对于 2020.12.0 版本，运行所有容器的单个实例的最低系统要求是：

- 6 个 CPU
- 26 GB RAM（最低 Redis 配置）；29 GB RAM（最佳配置），以便为 Redis 驱动的高速缓存提供更高的可用性
- 250 GB 可用磁盘空间，用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

对于 2020.12.0 版本，运行带有 Black Duck 二进制分析 的 Black Duck 所需的最低硬件为：

- 7 个 CPU
- 30 GB RAM（最低 Redis 配置）；33 GB RAM（最佳配置），以便为 Redis 驱动的高速缓存提供更高的可用性
- 350 GB 可用磁盘空间，用于数据库和其他 Black Duck 容器
- 数据库备份的相应空间

注：每个附加的 binaryscanner 容器都需要一个额外的 CPU、2 GB RAM 和 100 GB 可用磁盘空间。

日语

2020.8.0 版本的 UI、联机帮助和发行说明已本地化为日语。

版本 2020.10.0 中的新增功能和更改功能

新的自定义组件仪表板

为了便于您轻松查看对您至关重要的组件版本，在 2020.10.0 中，组件仪表板已根据您保存的组件搜索替换为自定义组件仪表板。 Black Duck 现在允许您使用各种属性搜索项目中使用的组件，保存搜索，然后使用“仪表板”页面从这些保存的搜索中查看仪表板。

对于每个组件版本，自定义组件仪表板显示以下信息：

- 使用此组件版本的项目版本数量以及每个项目版本的阶段、许可证、审查状态和安全风险
- 按风险类别划分的漏洞数量
- 许可证和运维风险
- 策略违反
- 审批状态
- 首次检测到组件版本的日期
- 根据 Black Duck KnowledgeBase 发布组件的日期
- 新版本的数量
- 组件的漏洞上次更新的日期

组件和 Black Duck KnowledgeBase 搜索增强功能

通过可用于搜索组件的属性以及搜索结果中显示的信息，可以增强组件搜索功能。UI 也得到了增强，因此您可以轻松区分对项目中使用的组件的搜索以及对 Black Duck KnowledgeBase 中的组件的搜索。

虽然 Black Duck KnowledgeBase 搜索的搜索属性未更改，但在搜索 Black Duck 项目中使用的组件版本时，以下属性可用：

- 安全风险
- 许可证风险
- 运维风险
- 策略规则
- 策略违反严重性
- 审核状态
- 组件审批状态
- 首次检测到
- 许可证系列
- 缺少自定义字段数据
- 发布日期
- 许可证
- 漏洞 CWE
- 漏洞报告日期

对于与搜索条件匹配的每个组件版本，将显示以下信息：

- 使用此组件版本的项目版本数量以及每个项目版本的阶段、许可证、审查状态和安全风险
- 按风险类别划分的漏洞数量
- 许可证和运维风险
- 策略违反
- 审批状态
- 首次检测到组件版本的日期
- 根据 Black Duck KnowledgeBase 发布组件的日期
- 新版本的数量
- 组件的漏洞上次更新的日期

现在可以保存这些组件搜索结果并在“仪表板”页面中查看，如上所述。

对于每个知识库组件搜索结果，将显示以下信息：

- 使用此组件的项目版本数以及每个项目版本、其阶段、使用的组件版本以及相关安全风险的列表
- 提交活动趋势
- 最后提交日期
- 组件版本数量
- 此组件的标记

保存的搜索的增强

Black Duck 现在可以在 “仪表板” 页面上过滤和排序已保存的搜索。

许可证冲突

在 2020.10.0 版本中，Black Duck 现在可以为您指定不兼容的自定义许可条款。您可以为与 Black Duck KnowledgeBase 条款或自定义许可条款冲突的禁止操作或必需操作定义自定义许可条款。

注: 目前，您无法在项目版本 BOM 中查看不兼容的许可条款。此功能将在将来的 Black Duck 版本中提供。

许可证管理增强

这三个新过滤器已添加到 “许可证管理” 中的许可条款选项卡中：

- 与许可证关联
- 有不兼容的条款
- 责任

新组件的用法

Black Duck 添加了一个 “未指定” 用法，您可以使用该用法表明您需要调查组件的用法。您可能会发现使用此用法作为默认值来替代现有默认值（比如 “动态链接” ）会非常有用，这样就可以消除混淆，能够分辨组件被分配了实际用法值还是默认值。

新层级

Black Duck 添加了一个层级 0，您可以使用它指定为最关键的层级。

由于此新层级，这些默认策略规则已修改为包括层级 0：

- 没有具有 1 个以上高风险漏洞的外部层级 0、层级 1 或层级 2 项目
- 没有具有 3 个以上中等风险漏洞的外部层级 0、层级 1 或层级 2 项目

现有层级没有变化。

自定义字段的增强

自定义字段有以下增强

- Black Duck 现在提供了让您指定自定义字段是必填项的功能。
  - 查看自定义字段信息时，会出现警告消息 “* 附加字段为必填项” 。但是，如果没有为必填的自定义字段输入数据，用户仍可以在页面上查看和保存非自定义字段信息和非必填自定义字段的信息。
  - BOM 中添加了一个新的过滤器 “缺少自定义字段数据” ，以便您可以查看项目版本 BOM 中缺少信息的组件。
- 添加了在查看布尔字段类型和单选字段类型的自定义字段信息时清除选择的选项。

允许的特征列表

特征列表定义了 Black Duck 发送到 Black Duck KnowledgeBase Web 服务的特征，以识别扫描代码中包含的开源软件。 特征扫描程序 现在有两个新参数，您可以使用它们为二进制文件扩展名或源文件扩展名创建允许的特征列表。每个列表都是可选的，并且与其他列表无关。

- --BinaryAllowedList x, y, x，其中 x、y、z 是 SHA-1（二进制）文件的批准文件扩展名。
- --SourceAllowedList a, b, c，其中 a、b、c 是干净 SHA-1（源代码）文件的批准扩展名。

漏洞影响分析的增强

对漏洞影响分析进行了以下增强：

- 在 security_date_time.csv 项目版本报告的末尾添加了一个新列“可访问”，以表示安全漏洞是可访问 (true) 还是不可访问 (false)。
- 已将新的过滤器“可访问”添加到项目版本的安全选项卡中。

报告增强

以下报告得到了加强：

- 在 components_date_time.csv 项目版本报告的末尾添加了一个新列“注释”，并列出了每个组件的注释。
- vulnerability-status-report_date_time.csv 报告末尾添加了一个新的“匹配类型”列，以标识匹配类型。

报告数据库的增强

以下列已添加到组件匹配表 (component_matches) 中：

- match_confidence。表示匹配的可信度，不包括代码段、二进制或部分文件匹配。
- match_archive_context。相对于项目根目录的存档文件的本地路径。
- snippet_confirmation_status。审查代码段匹配的状态。

HTTP/2 和 TLS 1.3

为了提高浏览器中 Black Duck UI 的安全性和渲染效果，Black Duck 现在在 Black Duck NGINX Web 服务器中支持 HTTP/2 和 TLS 1.3。请注意，Black Duck NGINX Web 服务器继续支持 HTTP/1.1 和 TLS 1.2。

对清除扫描的作业的更改

BomVulnerabilityNotificationJob 和 LicenseTermFulfillmentJob 现在也移除了旧的审核事件。

支持的浏览器版本

- Safari 版本 13.1.2 (14609.3.5.1.5)
- Chrome 版本 86.0.4240.80
- Firefox 82（64 位）
- Internet Explorer 11.572.19041.0

  请注意，对 Internet Explorer 11 的支持已弃用，Black Duck 将从 Black Duck 2021.2.0 版本开始停止对 Internet Explorer 11 的支持。
- Microsoft Edge 86.0.622.51（正式版本）（64 位）

容器版本

- 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

日语

2020.8.0 版本的 UI、联机帮助和发行说明已本地化为日语。

API 增强

- 添加了一个端点以确定 Black Duck 的单点登录 (SSO) 状态。

  GET /api/sso/status
- 添加了用于检索 SAML/LDAP 配置的端点（仅限管理员使用）。
  - 读取 SSO 配置：

    GET /api/sso/configuration
  - 下载 IDP 元数据文件：

    GET /api/sso/idp-metadata
  - 还添加了以下 SSO 端点：
    - 更新 SSO 配置：

      POST /api/sso/configuration
    - 上传 IDP 元数据文件：

      POST /api/sso/idp-metadata
- 添加了以下 BOM 分层组件端点：
  - 列出分层根组件：

    GET /api/projects/{projectId}/versions/{projectVersionId}/hierarchical-components
  - 列出分层子组件：

    GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/hierarchical-components/{hierarchicalId}/children
  - 列出分层子组件版本：

    GET/api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/hierarchical-components/{hierarchicalId}/children
- 在通知 API 中添加了新的漏洞字段，以便进一步分类通知。这些通知涉及 BOM 中已更改的漏洞信息，并包括以下字段：
  - vulnerabilityNotificationCause

有关发生并触发通知的漏洞事件类型的信息，比如漏洞已添加或删除、更改了注释、更改了修复详细信息、更改了漏洞严重性或状态已更改。

- eventSource

  有关生成通知的来源的信息，比如扫描、Black Duck KB 更新或用户操作（比如修复、优先级重新排序或调整）。

- /api/catalog-risk-profile-dashboard API 现在返回 HTTP 410 (GONE)。

修复了版本 2020.10.0 中的问题

在此发布中修复了客户报告的以下问题：

- （Hub-20559、22100）。修复了从不同根目录扫描相同代码位置或克隆项目版本时丢失代码段调整的问题。
- (Hub-21421)。修复了打印功能不适用于大型项目的问题。
- （Hub-23705、25560）。修复了用户无法删除其创建的报告的问题。
- (Hub-23709)。修复了扫描时出现以下 scan.cli.sh 警告消息的问题：“无法从所有清单中找到清单。”
- (Hub-24330)。修复了以下问题：在将 Protex 项目导入到 Black Duck 版本 2019.10.3 时出现错误消息（“重复密钥值违反了唯一限制”）。
- (Hub-24673)。修复了在组件数超过 32,000 的情况下从“仪表板”页面导航失败的问题。
- (Hub-24675)。修复了 root_bom_consumer_node_id 设置不正确的问题
- (Hub-24871)。修复了自 2019.10.0 发布以来 PostgreSQL 数据库增长的问题。
- (Hub-24772)。修复了打印 BOM 时默认 .pdf 文件名不是项目名称和版本名称的问题。
- (Hub-24839)。修复了无法从“添加/编辑组件”对话框中选择某些组件原始 ID 的问题。
- (Hub-24947)。修复了将项目添加到 BOM 时搜索结果的列出不一致的问题。
- (Hub-25171)。修复了在使用 API 修复漏洞时漏洞计数在重新扫描后才更新的问题 (PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/origins/{originId}/vulnerabilities/{vulnerabilityId}/remediation)。
- (Hub-25219)。修复了通过 API 创建报告时的问题，其中指定区域设置（比如“区域设置”：“ja_JP”）被忽略。现在，区域设置字段可以正确设置生成的报告的语言。
- (Hub-25234)。修复了打印 BOM 的打印按钮偶尔缺少条形图计数的问题。
- (Hub-25240)。修复了特定漏洞 (BDSA-2020-1674) 的浏览器或 API 调用失败的问题。
- (Hub-25241)。修复了 VersionBomComputationJob 扫描失败并显示以下错误消息的问题：“数据完整性违反（限制：not_null，详细信息：在列 source_start_lines 上）”。
- (Hub-25244)。修复了以下问题：在升级到 2020.4.2 版本 Black Duck 后从 BOM 中删除手动添加的组件。
- (Hub-25247)。修复了 Black Duck PostgreSQL 日志中出现以下错误消息的问题：“错误：重复密钥值违反了唯一限制 scan_component_scan_id_bdio_node_id_key”。
- (Hub-25321)。修复了滚动 BOM 页面时，文本出现在页面上不应显示文本的区域的问题。
- (Hub-25324)。修复了“扫描名称”页面没有换行的问题。
- (Hub-25478)。修复了“安全”页面上的安全风险过滤器变得不可见的问题。

- (Hub-25508)。修复了旧版媒体类型（v4 和 v5）并非始终适用于策略规则 API (GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/policy-rules) 的问题。
- （Hub-25522、25523）。修复了以下问题：对于 Black Duck 版本 2020.8.0，在 Chrome 的 BOM 打印预览窗口中出现格式错误。
- (Hub-25548)。修复了在分层视图中选择新组件匹配时不更新“来源”视图中的组件匹配的问题。
- (Hub-25570)。修复了“安全仪表板”页面仅部分加载的问题。
- (Hub-25608)。修复了漏洞更新报告中“新漏洞”和“新修复漏洞”类别中漏洞计数两次的问题。
- (Hub-25649)。修复了“仪表板”页面上的策略违反弹出窗口无法关闭的问题。
- (Hub-25841)。修复了输入到“文本”类型的自定义字段中的数字转换为日期格式的问题。

3. 已知问题和限制

以下是 Black Duck 中已知问题和限制的列表：

当前已知问题和限制

- 同时创建或更新多个基于持续时间的策略可能会导致 BOM 引擎容器内存不足并重启，具体取决于系统资源。如果发生这种情况，请联系客户支持寻求帮助。
- 由于安全排名算法更新，在“查找”→“漏洞”页面上搜索漏洞可能会显示与以前版本不同的结果。
- 将活动项目版本转换为 LTS 时，如果活动项目包括通过代码段扫描识别的组件，则可能会在 LTS 项目中发现额外漏洞。在未来的更新中，通过代码段扫描匹配的组件将不再转入到 LTS 项目。
- Bitbucket 数据中心的 SCM 集成目前无法正常运行。请联系 Black Duck 支持人员，获得有关使用此功能的协助。
- Bitbucket 云 SCM 提供商的用户必须在 Bitbucket 中使用相同的工作空间名称和工作空间 ID，才能从该工作空间克隆存储库。
- 在“查找”页面搜索 CISA 已知可利用漏洞时，您必须同时勾选“受影响的项目”复选框才能获得结果。仅勾选“CISA 已知可利用漏洞”复选框不会生成任何搜索结果。
- 在“管理”>“诊断”>“热图”下找到的扫描热图以 UTC 时间（而不是本地时间）显示结果。请在使用此新功能时注意这一点。
- 当通过 UI 重新上传 BDIO 时，基于匹配分数阈值设置标记为删除的组件没有被移除。
- 在项目（项目 > “设置”选项卡）和全局（管理 > 系统设置 > 数据保留）级别，仅清除存档项目版本未匹配的扫描文件数据和清除所有未匹配的文件数据链接都不起作用。
- 如果使用 LDAP 目录服务器对用户进行身份验证，请考虑以下事项：
  - Black Duck 支持单个 LDAP 服务器。不支持多个服务器。
  - 如果从目录服务器中移除用户，Black Duck 用户帐户将继续显示为活动状态。但是，凭据不再有效，无法用于登录。
  - 如果从目录服务器中移除组，Black Duck 组不会移除。手动删除组。
- 标记只支持字母、数字以及加号 (+) 和下划线 (_) 字符。
- 如果 Black Duck 正在对用户进行身份验证，则在登录期间用户名不区分大小写。如果启用了 LDAP 用户身份验证，则用户名区分大小写。
- 如果代码位置有大型材料清单，删除代码位置可能会失败，并出现用户界面超时错误。