



发行说明

版本 2022.2.0



此版本的 发行说明 指的是 Black Duck 的 2022.2.0 版本。

本文档在 2022年3月15日 创建或更新。

请将您的意见和建议发送至：

Synopsys
800 District Avenue, Suite 201
Burlington, MA 01803-5061 USA

版权所有 © 2022, 所有者：Synopsys。

保留所有权利。本文档的所有使用均受 Black Duck Software, Inc. 和被许可人之间的许可协议约束。未经 Black Duck Software, Inc. 事先书面许可，不得以任何形式或任何方式复制或传播本文档的任何内容。

Black Duck、Know Your Code 和 Black Duck 徽标是 Black Duck Software, Inc. 在美国和其他司法管辖区的注册商标。Black Duck Code Center、Black Duck Code Sight、Black Duck Hub、Black Duck Protex 和 Black Duck Suite 是 Black Duck Software, Inc. 的商标。所有其他商标或注册商标均为其各自所有者的独占财产。

CH: 章节 1: 产品公告	viii
版本 2022.2.0 的公告	viii
增强型特征生成	viii
API 请求的最大页数限制	viii
已弃用的 API	viii
即将对资源指导进行的更改	viii
日语	x
简体中文	x
版本 2021.10.3 的公告	x
Apache Log4J2 的安全顾问 (CVE-2021-45046 和 CVE-2021-45105)	x
版本 2021.10.2 的公告	xi
Apache Log4J2 的安全顾问 (CVE-2021-44228)	xi
版本 2021.10.0 的公告	xi
增强型特征扫描	xi
关于 Detect 7.4 和 Black Duck 2021.8.0 的说明	xi
PostgreSQL 容器从 9.6 迁移到 11	xi
Black Duck PostgreSQL 9.6 弃用	xi
PostgreSQL 支持时间表	xi
从 2021.10.0 开始, 数据库 bds_hub_report 弃用	xii
即将对 API 请求实施最大页面限制	xii
已弃用的 API	xii
日语	xiii
简体中文	xiii
版本 2021.8.7 的公告	xiii
Apache Log4J2 的安全顾问 (CVE-2021-45046 和 CVE-2021-45105)	xiii
版本 2021.8.6 的公告	xiii
Apache Log4J2 的安全顾问 (CVE-2021-44228)	xiii
版本 2021.8.0 的公告	xiii
Black Duck 2021.8.0 版本需要 Detect 7.4	xiii
CentOS-7 上的 Desktop Scanner	xiv
日语	xiv
简体中文	xiv
已弃用的 API	xiv

版本 2021.6.0 的公告	xiv
针对外部数据库的 PostgreSQL 版本 9.6 的支持终止	xiv
已弃用的页面	xiv
已弃用的 API	xiv
日语	xv
版本 2021.4.0 的公告	xv
新容器和系统要求更改	xv
未映射的代码位置的保留期	xvi
已弃用的 API	xvi
2021.6.0 版本中的新作业实施	xvi
日语	xvi
版本 2021.2.0 的公告	xvi
Azure 客户通知	xvi
对外部数据库弃用 PostgreSQL 版本 9.6	xvii
不再支持 Internet Explorer 11	xvii
已弃用的页面	xvii
日语	xvii
版本 2020.12.0 的公告	xvii
新容器和系统要求更改	xvii
终止对 Internet Explorer 11 的支持	xvii
日语	xviii
版本 2020.10.0 的公告	xviii
新容器和系统要求更改推迟到 2020.12.0 版本	xviii
日语	xviii
版本 2020.8.0 的公告	xviii
对外部数据库弃用 PostgreSQL 版本 9.6	xviii
2020.10.0 版本中的已弃用 API	xviii
日语	xix
版本 2020.6.1 的公告	xix
终止对 Internet Explorer 11 的支持	xix
版本 2020.6.0 的公告	xix
未来版本中的新容器和系统要求更改	xix
弃用 Internet Explorer 11 支持	xx
对外部数据库的 PostgreSQL 11 支持	xx
版本 2020.2.0 的公告	xx
单个文件匹配	xx
Docker Compose 支持	xx
CH: 章节 2: 版本信息	xxi
版本 2022.2.0	xxi
版本 2022.2.0 中的新增功能和更改功能	xxi
API 增强	xxvii

修复了 2022.2.0 中的问题	xxix
版本 2021.10.3	xxxii
版本 2021.10.3 中的新增功能和更改功能	xxxii
修复了 2021.10.3 中的问题	xxxii
版本 2021.10.2	xxxiii
版本 2021.10.2 中的新增功能和更改功能	xxxiii
修复了 2021.10.2 中的问题	xxxiii
版本 2021.10.1	xxxiv
版本 2021.10.1 中的新增功能和更改功能	xxxiv
修复了 2021.10.1 中的问题	xxxiv
版本 2021.10.0	xxxv
版本 2021.10.0 中的新增功能和更改功能	xxxv
API 增强	xxxvii
修复了 2021.10.0 中的问题	xxxviii
版本 2021.8.7	xxxix
版本 2021.8.7 中的新增功能和更改功能	xxxix
修复了 2021.8.7 中的问题	xl
版本 2021.8.6	xl
版本 2021.8.6 中的新增功能和更改功能	xl
修复了 2021.8.6 中的问题	xli
版本 2021.8.5	xli
版本 2021.8.5 中的新增功能和更改功能	xli
修复了 2021.8.5 中的问题	xli
版本 2021.8.4	xlii
版本 2021.8.4 中的新增功能和更改功能	xlii
修复了 2021.8.4 中的问题	xlii
版本 2021.8.3	xliii
版本 2021.8.3 中的新增功能和更改功能	xliii
修复了 2021.8.3 中的问题	xliii
版本 2021.8.2	xliv
版本 2021.8.2 中的新增功能和更改功能	xliv
修复了 2021.8.2 中的问题	xliv
版本 2021.8.1	xlvi
版本 2021.8.1 中的新增功能和更改功能	xlvi
修复了 2021.8.1 中的问题	xlvi
版本 2021.8.0	xlvi
版本 2021.8.0 中的新增功能和更改功能	xlvi
修复了 2021.8.0 中的问题	xlix
版本 2021.6.2	l
版本 2021.6.2 中的新增功能和更改功能	l
修复了 2021.6.2 中的问题	li

版本 2021.6.1	li
版本 2021.6.1 中的新增功能和更改功能	li
修复了 2021.6.1 中的问题	lii
版本 2021.6.0	lii
版本 2021.6.0 中的新增功能和更改功能	lii
修复了 2021.6.0 中的问题	lvii
版本 2021.4.1	lviii
版本 2021.4.1 中的新增功能和更改功能	lviii
修复了 2021.4.1 中的问题	lviii
版本 2021.4.0	lviii
版本 2021.4.0 中的新增功能和更改功能	lviii
修复了 2021.4.0 中的问题	lxiii
版本 2021.2.1	lxiv
版本 2021.2.1 中的新增功能和更改功能	lxiv
修复了 2021.2.1 中的问题	lxv
版本 2021.2.0	lxv
版本 2021.2.0 中的新增功能和更改功能	lxv
修复了 2021.2.0 中的问题	lxx
版本 2020.12.0	lxxi
版本 2020.12.0 中的新增功能和更改功能	lxxi
修复了 2020.12.0 中的问题	lxxv
版本 2020.10.1	lxxvi
版本 2020.10.1 中的新增功能和更改功能	lxxvi
修复了 2020.10.1 中的问题	lxxvi
版本 2020.10.0	lxxvi
版本 2020.10.0 中的新增功能和更改功能	lxxvi
修复了 2020.10.0 中的问题	lxxxi
CH: 章节 3: 已知问题和限制	lxxxiii
新的已知问题	lxxxiii
当前已知问题和限制	lxxxiii

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。
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 Synopsysctl 和 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。
- [Synopsysctl](#) 是一款云原生管理命令行工具，用于在 Kubernetes 和 Red Hat [OpenShift](#) 中部署 Black Duck 软件。

Black Duck 集成文档可在 [Confluence](#) 上找到。

客户支持

如果您在软件或文档方面遇到任何问题，请联系 Synopsys 客户支持。

您可以通过以下几种方式联系 Synopsys 支持：

- 在线: <https://www.synopsys.com/software-integrity/support.html>
- 电话: 请参阅我们的 [支持页面](#) 底部的“联系我们”部分以查找您当地的电话号码。

要打开支持案例, 请登录 Synopsys Software Integrity 社区网站, 网址为: <https://community.synopsys.com/s/contactsupport>。

另一个可随时使用的方便资源是 [在线客户门户](#)。

Synopsys Software Integrity 社区

Synopsys Software Integrity 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 Software Integrity Group (SIG) 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 SIG 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 Synopsys 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 SIG 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 Software Integrity Group 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@synopsys.com。

培训


Synopsys Software Integrity 的客户教育 (SIG Edu) 板块是满足您的所有 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 Synopsys Software Integrity 的客户教育 (SIG Edu) 板块, 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://community.synopsys.com/s/education>, 或者从 Black Duck UI 的“帮助”

菜单 () 中选择 **Black Duck 教程** 获取 Black Duck 的帮助信息。

Synopsys 关于包容性和多样性的声明

Synopsys 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。

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, 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** 增强部分。

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。

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 版的 UI、联机帮助和发布说明已本地化为日语。

简体中文

2021.10.0 版的 UI、联机帮助和发行说明已本地化为简体中文。

版本 2021.10.3 的公告

Apache Log4j2 的安全顾问 (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 Synopsys 的产品、服务和系统的曝光度有限。根据我

们所遇到的情况，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 2021.10.2 的公告

Apache Log4j2 的安全顾问 (CVE-2021-44228)

Synopsys 意识到与名为 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 Synopsys 的产品、服务和系统的曝光度有限。根据我们所遇到的情况，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.synopsys.com/blogs/software-security/zero-day-exploit-log4j-analysis/>

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 Synopsys 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

在 2022.2.0 版本中，Black Duck 会将其 PostgreSQL 映像从版本 9.6 迁移到版本 11。不使用 Synopsys 提供的 PostgreSQL 映像的客户不会受到影响。

Black Duck PostgreSQL 9.6 弃用

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	最后发布	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 开始, 数据库 bds_hub_report 弃用

从 2021.10.0 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 版的 UI、联机帮助和发布说明已本地化为日语。

简体中文

2021.8.0 版的 UI、联机帮助和发行说明已本地化为简体中文。

版本 2021.8.7 的公告

Apache Log4J2 的安全顾问 (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 Synopsys 的产品、服务和系统的曝光度有限。根据我们所遇到的情况, 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 2021.8.6 的公告

Apache Log4J2 的安全顾问 (CVE-2021-44228)

Synopsys 意识到与名为 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 Synopsys 的产品、服务和系统的曝光度有限。根据我们所遇到的情况, 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.synopsys.com/blogs/software-security/zero-day-exploit-log4j-analysis/>

版本 2021.8.0 的公告

Black Duck 2021.8.0 版本需要 Detect 7.4

Black Duck 版本 2021.8.0 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 Electron12 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 版的 UI、联机帮助和发布说明已本地化为日语。

简体中文

2021.2.0 版的 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 2021.6.0 的公告

针对外部数据库的 PostgreSQL 版本 9.6 的支持终止

从 Black Duck 2021.6.0 版本开始, 对于外部数据库, Synopsys 已终止支持 PostgreSQL 版本 9.6。

对于外部数据库, Black Duck 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 版的 UI、联机帮助和发布说明已本地化为日语。

版本 2021.4.0 的公告

新容器和系统要求更改

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** 知识库的连接，并以较短的时间间隔缓存知识库结果。

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)，可为 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)，可为 Redis 驱动的高速缓存提供更高的可用性。这将支持超过 150 个快速扫描，但支持的最大快速扫描数仍在确定中。
- 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)，可为 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)，可为 Redis 驱动的高速缓存提供更高的可用性。这将支持超过 150 个快速扫描，但支持的最大快速扫描数仍在确定中。
- 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

注意：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, 以下端点将被弃用:

```
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** 中将保持无效。

- **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 **Job 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 版的 UI、联机帮助和发布说明已本地化为日语。

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

从 Black Duck 2021.6.0 版本开始, Synopsys 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

Synopsys 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 版的 UI、联机帮助和发布说明已本地化为日语。

版本 2020.12.0 的公告

新容器和系统要求更改

还有两个附加容器: 2020.12.0 版的 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), 可为 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), 可为 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

注意: 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, Synopsys 将从 Black Duck 2021.2.0 发布开始停止对 Internet Explorer 11 的支持。

日语

2020.10.0 版的 UI、联机帮助和发布说明已本地化为日语。

版本 2020.10.0 的公告

新容器和系统要求更改推迟到 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。

对于 2020.12.0 版, 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), 可为 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, 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), 可为 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

注意: 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 版的 UI、联机帮助和发布说明已本地化为日语。

版本 2020.8.0 的公告

对外部数据库弃用 PostgreSQL 版本 9.6

从 **Black Duck** 2021.6.0 版本开始, Synopsys 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。

2020.10.0 版本中的已弃用 API

在 **Black Duck** 2020.10.0 版本中, /api/catalog-risk-profile-dashboard API 将返回 HTTP 410 (GONE), 从 **Black Duck** 2020.12.0 版本开始, 此 API 将不可用。

将在 2020.10.0 版本中公布一个新的 API 来取代 /api/catalog-risk-profile-dashboard。

日语

2020.6.0 版的 UI、联机帮助和发布说明已本地化为日语。

版本 2020.6.1 的公告

终止对 Internet Explorer 11 的支持

对 Internet Explorer 11 的支持已弃用, Synopsys 将从 Black Duck 2021.2.0 发布开始停止对 Internet Explorer 11 的支持。

版本 2020.6.0 的公告

未来版本中的新容器和系统要求更改

2020.8.0 版本

在 **2020.8.0 版本**中, 将在 Black Duck 中添加新的 Redis 容器。此容器将在 Black Duck 中实现更一致的缓存功能, 并将用于提高应用程序性能。

以下是运行所有容器的单个实例所需的最低硬件:

- 5 个 CPU
- 21 GB RAM(最低 Redis 配置); 24 GB RAM(最佳配置), 可为 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

以下是运行带有 Black Duck - 二进制分析 的 Black Duck 所需的最低硬件:

- 6 个 CPU
- 25 GB RAM(最低 Redis 配置); 28 GB RAM(最佳配置), 可为 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

注意: 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。

2020.10.0 版本

在 **2020.10.0 版本**中, Black Duck 将添加两个附加容器: BOM 引擎和 RabbitMQ(将是必需的容器)。这些容器将用于提高应用程序性能, 主要是提高项目版本 BOM 性能。

初始测试表明, 运行所有容器的单个实例的最低系统要求如下:

- 6 个 CPU
- 26 GB RAM(最低 Redis 配置); 29 GB RAM(最佳配置), 可为 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

初始测试表明, 运行带有 Black Duck - 二进制分析 的 Black Duck 所需的最低硬件将是:

- 7 个 CPU
- 30 GB RAM(最低 Redis 配置); 33 GB RAM(最佳配置), 可为 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

注意: 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。

请注意, 这些系统要求基于初始测试结果。最终系统要求可能低于此处所示的要求, 但不会超过此处列出的要求。

弃用 Internet Explorer 11 支持

从 Black Duck 2021.2.0 版本开始, Synopsys 将不再支持 Internet Explorer 11。

对外部数据库的 PostgreSQL 11 支持

对于使用外部 PostgreSQL 的新安装, Black Duck 现在支持 PostgreSQL 11.7。尽管外部 PostgreSQL 实例仍然完全支持 PostgreSQL 9.6, 但 Synopsys 建议使用外部 PostgreSQL 的新安装使用 PostgreSQL 11.7。

对于内部 PostgreSQL 容器的用户, PostgreSQL 9.6 仍然是 Black Duck 2020.6.0 支持的版本。

版本 2020.2.0 的公告

单个文件匹配

如前所述, 为了减少由于不明确匹配而导致的误报, 作为特征扫描的一部分执行单个文件匹配不再是 Black Duck CLI 和 Synopsys Detect 扫描的默认行为。

单个文件匹配是纯粹基于单个文件的校验和信息来识别组件。在 Black Duck 中, 对于一小组文件扩展名(.js、.apklib、.bin、.dll、.exe、.o 和 .so), 常规特征扫描根据与一个文件的校验和匹配将文件与组件匹配。不幸的是, 这种匹配并不总是准确的, 并且产生了相当多的误报。为了改善整个 Synopsys 客户群的整体开发人员体验, 单个文件匹配不再是默认行为, 现在它是可选功能。

升级到 2020.2.0 将关闭单个文件匹配, 并可能导致某些组件从 BOM 上丢失。要估计对 BOM 的影响, 请查找仅具有“精确文件”匹配类型的组件, 以查看可能从 BOM 中丢失的组件。请注意, 如果您正在扫描 Docker 映像, “精确文件”匹配不受此更改的影响。

特征扫描程序 具有一个新参数用于启用单个文件匹配。如果您使用 Synopsys Detect 进行扫描, 6.2 版将有一个新参数, 支持打开/关闭单个文件匹配, 默认值为“关闭”。

Docker Compose 支持

如前所述, Docker Compose 不再是 2020.2.0 版本支持的编排方法。

版本 2022.2.0

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 PostgreSQL 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 Synopsys 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:

```
kubectrl 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 Synopsys 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 and 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 安全顾问 (BDSA) 团队将 <漏洞 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 <漏洞 ID> 映射到此组件版本, 但 Black Duck 安全顾问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~
{projectId}。

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。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)(64 位)
 - 不再支持 Microsoft Edge 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
- sigsynopsys/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`
- `BINARY`
- `BOM_IMPORT`
- `SIGNATURE`

传统扫描仍将使用 `BDIO` 作为 `scanType` 值。

请注意, 此更改是在 **Black Duck 2021.8.0** 中引入的。

修复了 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)。修复了知识库活动作业的问题, 这些知识库活动作业处理组件、组件版本、许可证、NVD 漏洞和 BDSA 漏洞的知识库更新。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完成, 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 KBUUpdateWorkflow 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/操作风险。
- (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。

版本 2021.10.3

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
- sigsynopsys/bdba-worker:2021.9.2
- blackducksoftware/rabbitmq:1.2.5

修复了 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

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
- sigsynopsys/bdba-worker:2021.9.2
- blackducksoftware/rabbitmq:1.2.5

修复了 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

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知识库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
- sigsynopsys/bdba-worker:2021.9.1
- blackducksoftware/rabbitmq:1.2.5

修复了 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

版本 2021.10.0 中的新增功能和更改功能

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。

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 **Admin**, 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:

- 1.1 版本有 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
- 1.2 版本有 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。

注意: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

现在, Black Duck 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。

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)(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
- sigsynopsys/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

现在, **Black Duck** 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服务于 **Copyright 1.0**(也称“传统”)数据:

```
GET /api/components/{componentId}/versions/{componentVersionId}/origin/{originId}/file-copyrights-legacy
```

注意:这个新端点不能直接在 **Black Duck UI** 中使用, 而是直接通过公共 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 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, 以便在 SAML SSO 用户登录失败时显示便于理解的错误消息。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。

版本 2021.8.7

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
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

修复了 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

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
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

修复了 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

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。

修复了 2021.8.5 中的问题

- (HUB-31482)。修复了 Black Duck 版本 2021.6.2 之后 Snippet 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。

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
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

版本 2021.8.4

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。

修复了 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。

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
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

版本 2021.8.3

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`

修复了 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)。修复了一个问题:在更新上传源信息之前,有时会完成极小的代码位置代码段扫描,从而显示上传的源丢失。

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
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

版本 2021.8.2

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。

修复了 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 **README.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。

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
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

版本 2021.8.1

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。

修复了 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 的问题。之前的其他版本不受影响。

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
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

版本 2021.8.0

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

对于使用外部 PostgreSQL 的新安装, Black Duck 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。

注意: 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

现在, **Black Duck** 可以在 **Hub** 中对所有项目进行逻辑分组, 从而使您可以整理出哪个项目属于哪个业务部门, 从而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”。

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 Media Type: 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

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
- sigsynopsys/bdba-worker:2021.7.0
- blackducksoftware/rabbitmq:1.2.3

修复了 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)。修复了一个问题:如果 BOM 有两个具有完全相同的名称、但 UUID 不同的组件, 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)。修复了一个问题:在“项目版本”>“详细信息”视图中,“更新时间”(或 2021.8.0 中的“上次设置更新”)时间戳(而非更新者用户名)将被更新。“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)。修复了一个问题:上传与项目有关系的 **bdio** 文件时, 如果该文件也位于“**bdio** 树”下部, 则该文件不可见。
- (HUB-29481)。修复了一个问题:通知报告中省略了名称相同、但使用不同大写字母的许可证。
- (HUB-30143)。修复了一个问题:**Protex BOM** 工具 **2021.6.0** 无法与最新的 **JDK (11.0.11)** 配合使用。
- (HUB-29274)。修复了一个问题:在 **BOM** 页面上存在循环引用时, **VersionReportJob** 可能导致 **jobrunner**“内存不足”问题。
- (HUB-29381)。修复了一个问题:当项目版本添加为组件(使用“添加”>“项目”)时, 组件条目将显示无效的操作风险级别。
- (HUB-30087)。修复了一个问题: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)。修复了一个问题:针对节点文件运行 **Detect** 时特征扫描程序卡住。
- (HUB-25592)。修复了一个问题:自动从 **BOM** 中删除了零部件(或零部件版本)调整。
- (HUB-25552)。修复了一个问题:自动从 **BOM** 中添加/删除了具有“匹配”类型调整的组件(或组件版本)。
- (HUB-29196)。修复了一个问题:单击策略违反弹出窗口时, 窗口未消失, 且鼠标光标快速移离策略违反符号。
- (HUB-29573)。修复了一个问题:在查看策略违反模式时, 忽略了策略规则描述中的换行符。
- (HUB-30611)。修复了一个问题:数字用户名导致数据库迁移脚本出错。
- (HUB-26611)。修复了一个问题:在 **Detect** 中使用聚合时, 未正确报告直接/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)。修复了一个问题:**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。

版本 2021.6.2

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
- sigsynopsys/bdba-worker:2021.06
- blackducksoftware/rabbitmq:1.2.2

修复了 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)。修复了一个问题：由于在 NGINX 配置中为警报指定了代理证书位置，托管用户无法访问 Blackduck 警报实例。

版本 2021.6.1

版本 2021.6.1 中的新增功能和更改功能

Black Duck 安全顾问 (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 标记，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
- sigsynopsys/bdba-worker:2021.06
- blackducksoftware/rabbitmq:1.2.2

修复了 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)。修复了一个问题：2021.4.0 的二进制扫描容器 (bdba-worker) 无法通过增加超时和重试值在 docker SWARM 上运行。
- (HUB-29405)。修复了一个问题：因识别 core_i7 结构而导致匹配丢失。
- (HUB-30134)。修复了一个问题：由于 RabbitMQ 连接问题，导致 BOM 引擎静默启动失败。
- (HUB-30170)。修复了一个问题：利用双堆栈 Kubernetes 时，由于 docker 入口点配置不正确，导致 Redis 无法启动。
- (HUB-30202)。修复了一个问题：当用户单击 BDSA 评分，然后单击 NVD 评分时，“漏洞详细信息”页面无法正确更改得分指标的显示，反之亦然。

版本 2021.6.0

版本 2021.6.0 中的新增功能和更改功能

新容器和系统要求更改

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。
- 快速扫描功能现在可供所有 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 知识库的连接，并以较短的时间间隔缓存知识库结

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), 可为 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), 可为 Redis 驱动的高速缓存提供更高的可用性。这将支持超过 150 个快速扫描, 但支持的最大快速扫描数仍在确定中。

- 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), 可为 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), 可为 Redis 驱动的高速缓存提供更高的可用性。这将支持超过 150 个快速扫描, 但支持的最大快速扫描数仍在确定中。

- 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

注意: 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 的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 **Synopsys 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 BOM 计算, 并启动必要的作业。
 - **BomVulnerabilityDataRecomputationJob**. 更新从知识库收到的组件信息。
 - **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**. 启动从知识库收到的更新。
 - **KbUpdateWorkflowJob**-BDSA 漏洞更新。更新从知识库收到的 BDSA 漏洞信息。
 - **KbUpdateWorkflowJob**-组件更新。更新从知识库收到的组件信息。
 - **KbUpdateWorkflowJob**-组件版本更新。处理从知识库收到的组件版本更新。
 - **KbUpdateWorkflowJob**-许可证更新。更新从知识库收到的许可证信息。
 - **KbUpdateWorkflowJob**-NVD 漏洞更新。更新从知识库收到的 NVD 漏洞信息。
 - **KbUpdateWorkflowJob**-摘要。发布有关最新知识库更新的摘要报告。
 - **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 知识库版权信息的能力

现在, Black Duck 使您能够查看组件来源的更新 Black Duck 知识库版权信息。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

现在, Black Duck 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。

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 中将保持无效:
 - 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 Job 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。

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)(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
- sigsynopsys/bdba-worker:2021.03
- blackducksoftware/rabbitmq:1.2.2

日语

2021.4.0 版的 UI、联机帮助和发布说明已本地化为日语。

修复了 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)。修复了一个问题：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，以便在 SAML SSO 用户登录失败时显示便于理解的错误消息。
- (Hub-27209)。修复了一个问题：VersionBomComputationJob 失败并显示以下错误：“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)。修复了一个问题，以便在新的 Black Duck 搜索中将重置设为 0。
- (Hub-28171)。修复了一个问题：一个项目的版权搜索失败。
- (Hub-28305)。修复了一个问题：日志中出现以下错误：类 com.blackducksoftware.job.integration.domain.impl.JobMaintenanceJob 失败。
- (Hub-28347)。修复了一个问题：代码段调整导致重复密钥 SnippetAdjustment 错误。
- (Hub-28351)。修复了保存 BOM 许可证更改时的性能问题。
- (Hub-28469)。修复了一个问题：无法使用 Docker 20.10.x 配置自定义证书。
- (Hub-28726)。修复了一个问题：克隆项目后，Black Duck 将克隆项目的用户名显示为组件审查

者的名称。

- (Hub-28909)。修复了一个问题: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)。修复了一个问题:如果扫描中没有映射到项目版本的匹配项,则不会对该项目版本应用项目级文件调整。

版本 2021.4.1

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 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)。修复了一个问题:批量代码段调整失败并显示以下错误:“调整失败:服务器遇到错误, 请检查您的连接并重试。”
- (Hub-28807)。修复了一个问题: **Artifactory** 插件中出现以下错误:“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)。修复了一个问题:在“代码段确认”窗口中对未忽略的代码段进行筛选时, 显示了全系统范围内的代码段。
- (Hub-29448)。修复了一个问题: **LDAP** 用户授权失败并显示 `IncorrectResultSizeDataAccessException` 错误。

版本 2021.4.0

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 的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 **Synopsys 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。

注意: 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 **Synopsys** 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 **Synopsys 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

在编辑知识库或自定义组件版本的许可证时, **Black Duck** 现在使您能够在根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

现在, **Black Duck** 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** 知识库超时错误。

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,您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。

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

- 添加了 /api/component-migrations 和 /api/component-migrations/{componentOrVersionId} 端点, 以便根据特定日期或知识库中的特定组件获取组件迁移数据。
- 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。

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)(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
- sigsynopsys/bdba-worker:2021.03
- blackducksoftware/rabbitmq:1.2.2

日语

2021.2.0 版的 UI、联机帮助和发布说明已本地化为日语。

修复了 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)。修复了一个问题：在 UCS-2 编码文件的“代码段视图”对话框中出现红点，导致无法阅读文本。
- (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)。修复了一个问题：重复记录导致以下错误消息出现在 **job runner** 日志中：“冲突对象已存在。”
- (Hub-26481)。修复了一个问题：保存新的修复状态后页面将完全刷新。
- (HUB-26588)。修复了一个问题：在 **android-studio-ide-201.7199119-windows.exe** 上运行二进制扫描失败。
- (Hub-26695)。修复了一个问题：在一天中某些时间，扫描所用时间显著增加。
- (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)。修复了一个问题：选择替代代码段匹配时，会错误地将组件标识为具有加密。
- (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。

注意：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)。修复了一个问题：分配给具有全局项目查看者角色的非活动组的活动用户可以在“仪表板”中查看所有项目。
- (Hub-27175)。修复了一个问题：组件名称页面上的**已用计数**值不准确，因为它基于组件来源的数量，而不是组件版本。
- (Hub-27282)。修复了一个问题：BOM 中的策略违反弹出窗口有时卡在打开状态且无法关闭（除非刷新页面）。
- (Hub-27284、27660)。修复了一个问题：一些具有过渡依赖关系匹配类型的动态链接组件在项目版本 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)。修复了一个问题：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)。修复了一个问题：在“通知报告”中按区分大小写的顺序列出组件。

- (Hub-27308)。修复了一个问题:组件版本许可证更改后, **Black Duck KB 组件名称**页面未正确显示漏洞数量。
- (Hub-27326)。修复了一个问题:使用项目的**设置**选项卡删除应用程序 ID 时, 实际上未删除应用程序 ID。
- (Hub-27613)。修复了一个问题:无法在**来源**选项卡中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)。修复了一个问题: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)。修复了一个问题:在 **Black Duck** 构建 BOM 时会出现消息, 当您向下滚动 BOM 页面时, 该消息将消失。
- (Hub-28094)。修复了一个问题:/api/usergroups 端点在搜索词中未正确使用“_”或“%”。
- (Hub-28165)。修复了一个问题:在 BOM 页面上编辑许可证时, 在该页面上选择“取消/关闭”后, 仍会应用更改。
- (Hub-28208)。修复了一个问题:“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, 现在违反一个或多个策略的组件将在引入它们的代码位置未映射或被删除时生成“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)。修复了一个问题:HELM T 恤尺寸 .yaml 文件未扩展 BOM 引擎容器。
- (Hub-28370)。修复了一个问题: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)。修复了一个问题: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)。修复了一个问题:无法修改一组许可证的 AND 或 OR 运算符。
- (Hub-28458)。修复了一个问题:SnippetScanAutoBom 作业显示“作业执行错误:重复密钥”错误消息。
- (Hub-28562)。修复了一个问题:二进制扫描无法完成后期工作并显示以下错误消息:“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)。修复了一个问题:如果项目名称包含英文和中文字符, 则下载的报告文件后缀具有 .json 扩展名, 而不是 .zip。
- (Hub-28681)。修复了一个问题, 以便匹配类型为直接或过渡依赖关系时, **来源**选项卡上显示用法。
- (Hub-28765)。修复了一个问题:BOM 页面显示已确认和忽略的代码段。
- (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。

版本 2021.2.1

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 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)。修复了一个问题：重新扫描后，会更改已确认的代码段匹配。
- (Hub-26898)。修复了一个问题：似乎已完成扫描，但 Synopsys Detect 超时，因为它无法从 Black Duck 获得 bom_complete 通知。
- (Hub-27688)。修复了一个问题：匹配文件的 API 调用不返回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)。修复了一个问题：“产品注册”页面上显示错误的代码库大小。
- (Hub-28278)。修复了一个问题：RabbitMQ 容器缺少持久性卷，导致 BOM 引擎中创建过多的日志记录以及扫描失败。
- (Hub-28292)。修复了缩放 BOM 引擎容器的问题。

版本 2021.2.0

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 知识库中使用的漏洞，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 知识库中的漏洞。

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 **Synopsys 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`。高操作风险的数量。
- `operational_medium_count`。中等操作风险的数量。
- `operational_low_count`。低操作风险的数量。
- `operational_ok_count`。无操作风险的数量。

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** 现在使您能够在根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** 知识库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

要轻松查看 **Black Duck** 培训，您现在可以从 **Black Duck UI** 的“帮助”菜单 () 中选择 **Black Duck 教程**。

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。

Synopsys Detect 的托管位置

外部连接受限的 **Black Duck** 客户现在可以定义 **Synopsys 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) (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
- sigsynopsys/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。

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](/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 Synopsys Detect URI 端点, 仅用于设置或更新读取“系统设置”页面上的 Synopsys Detect

URI:

/external-config/detect-uri

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 版的 UI、联机帮助和发布说明已本地化为日语。

修复了 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 Black Duck 服务器在更新许可证状态时没有及时响应的问题。
- (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)。修复了除非重新启动 Black Duck，否则 SAML 的初始配置不会生效的问题。
- (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”类别的问题。
- (Hub-27208)。修复了在配置 SAML 时, Synopsys Alert 无法加载的 blackduck-nginx 问题。
- (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。

版本 2020.12.0

版本 2020.12.0 中的新增功能和更改功能

新容器和系统要求更改

还有两个附加容器:2020.12.0 版的 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),可为 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),可为 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

注意: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

注意: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, Synopsys 将从 Black Duck 2021.2.0 发布开始停止对 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
- sigsynopsys/bdba-worker:2020.09-1
- blackducksoftware/rabbitmq:1.2.2

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)”。

日语

2020.10.0 版的 UI、联机帮助和发布说明已本地化为日语。

修复了 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，以便在**来源**选项卡中查看许可证搜索结果页面时，在选择许可证类型时自动添加**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，以便在选择替代路径时刷新**来源**选项卡上“代码段视图”对话框中**匹配的文件路径**字段中显示的路径。
- (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。

版本 2020.10.1

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
- sigsynopsys/bdba-worker:2020.09-1
- blackducksoftware/rabbitmq:1.2.2

修复了 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 Synopsys 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

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
- 许可证和操作风险
- 策略违反
- 审批状态
- 首次检测到组件版本的日期
- 根据 **Black Duck** 知识库发布组件的日期
- 新版本的数量
- 组件的漏洞上次更新的日期

组件和 **Black Duck** 知识库搜索增强

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的使用的组件的搜索以及对 **Black Duck** 知识库中的组件的搜索。

虽然 **Black Duck** 知识库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
- 操作风险
- 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
- 许可证和操作风险
- 策略违反

- 审批状态
- 首次检测到组件版本的日期
- 根据 **Black Duck** 知识库发布组件的日期
- 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** 知识库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。

注意: 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** 发布中提供。

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 知识库 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, z**, 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列“匹配类型”, 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。

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)。

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, Synopsys 将从 Black Duck 2021.2.0 发布开始停止对 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
- sigsynopsys/bdba-worker:2020.09
- blackducksoftware/rabbitmq:1.2.2

日语

2020.8.0 版的 UI、联机帮助和发布说明已本地化为日语。

修复了 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”)的问题。
- (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 创建报告时的错误，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)。修复了在升级到 2020.4.2 版 **Black Duck** 后从 BOM 中删除手动添加的组件的问题。
- (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的问题。
- (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。

以下是 **Black Duck** 中已知问题和限制的列表：

新的已知问题

检测参数不兼容

请注意，当前使用 **Blackduck 2021.8.0** 或更高版本的客户在请求中使用以下参数调用 **Detect** 时可能会遇到超时问题：

- `--detect.wait.for.results=true`
- `--min-scan-interval=` (非零正值)

此问题将在即将发布的 **Detect** 和 **Blackduck** 版本中得到解决。

当前已知问题和限制

- 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。