BLACKDUCK

BY SYNOPSYS®

Getting Started

Version 2019.12.0

This edition of the *Getting Started* refers to version 2019.12.0 of Black Duck.

This document created or updated on Wednesday, December 11, 2019.

Please send your comments and suggestions to:

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

Contents

Black Duck documentation

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

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

Title	File	Description
Report Database	report_db.pdf	Contains information on using the report database.
User Guide	user_guide.pdf	Contains information on using Black Duck's UI.

Black Duck integration documentation can be found on Confluence.

Customer support

If you have any problems with the software or the documentation, please contact Synopsys Customer Support.

You can contact Synopsys Support in several ways:

- Online: https://www.synopsys.com/software-integrity/support.html
- Email: software-integrity-support@synopsys.com
- Phone: See the Contact Us section at the bottom of our support page to find your local phone number.

Another convenient resource available at all times is the online customer portal.

Synopsys Software Integrity Community

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

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

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

Training

Synopsys Software Integrity, Customer Education (SIG Edu) is a one-stop resource for all your Black Duck education needs. It provides you with 24x7 access to online training courses and how-to videos.

New videos and courses are added monthly.

At Synopsys Software Integrity, Customer Education (SIG Edu), you can:

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

Learn more at https://community.synopsys.com/s/education.

Chapter 1: Logging in to Black Duck

Black Duck is a risk management tool designed to help you manage the logistics of using open source software in your organization.

Using Black Duck, you can:

- Scan your code and identify open source software that exists in your code base.
- View the generated Bill of Materials (BOM) for your software projects.
- View vulnerabilities that have been identified in open source components.
- Assess your security, license, and operational risk.

Logging in to Black Duck lets you search projects that may be restricted to team members or company employees.

Note: You must have a username and password to access Black Duck. Contact your system administrator if you do not have a username. If Black Duck is configured to use LDAP, you may be able to log in to Black Duck using those credentials.

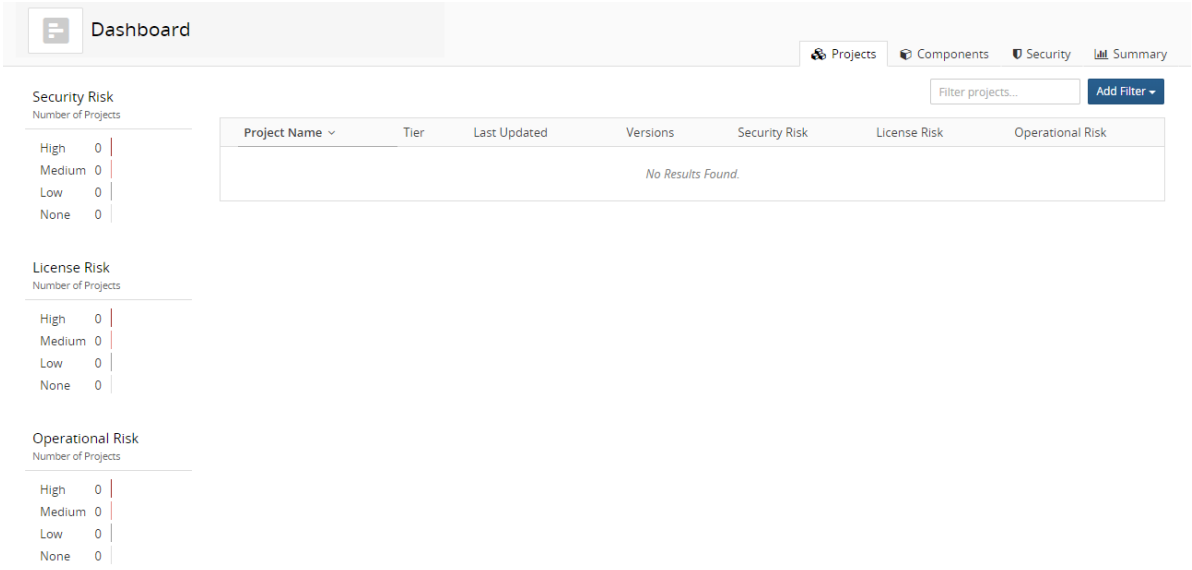
To log in to Black Duck

1. Using a browser, navigate to the Black Duck URL supplied by your system administrator. Typically the URL is in the format https://<server hostname>.
2. Enter the username and password provided by your Black Duck administrator.

   Note: Your password is case sensitive.

3. Click **Login**.

   When you log in, Black Duck displays your dashboard page.



When you first log in after installing Black Duck, an empty dashboard page appears. For information to appear in Black Duck, you need to scan your code and map your code to a project.

Chapter 2: Scanning your code

Black Duck component scanning is scanning functionality that provides an automated way to determine the set of open source software (OSS) components that make up a software project. Component scanning helps organizations manage their use of open source binaries by identifying and cataloging OSS components in order to provide additional metadata such as license, vulnerability, and OSS project health for those components.

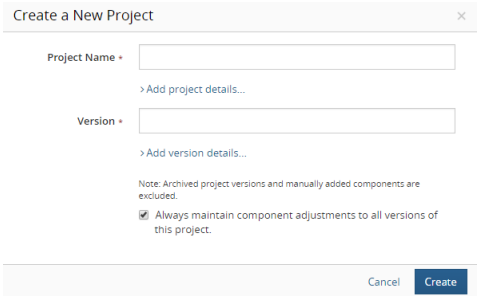
Creating a project

A project is the base unit in Black Duck. A project can be both a stand-alone development project and part of another project. For example, Apache Tomcat is a project in its own right but it may also be part of other, larger projects. You must create the projects that you want to make available for search by other developers in your organization.

Note that a project or application is limited to 10GB of Managed Code base.

To create a project

1. Log in to Black Duck.
2. Click **+ Create Project** at the top of any page.



3. In the Create a New Project dialog box, enter a project name. This name must be unique among projects in Black Duck, although it can have the same name as a project in the Black Duck KB.

Tip: As a best practice, you should think about how other users will search for your projects when creating project names. For example, if your project is related to 3D graphics, naming it "3DGraphics" means that the user must type the entire project name in order to find your project. If you use a space or an underscore in the name, for example, "3D Graphics" or "3D_Graphics", the additional separator characters will allow users to locate the project using the search term "3D".

4. Optionally, select **Add project details** to enter additional information such as:

   - Description.

     Tip: As a best practice, you should think about how other users will search for your projects when creating project descriptions. The description should be specific about what the project does and how it is unique, so that it is easily distinguishable from other similar projects.

   - Name of the project owner in the **Owner** field.

     Note: If the user you add is not already a project member, Black Duck adds the user to the project team.

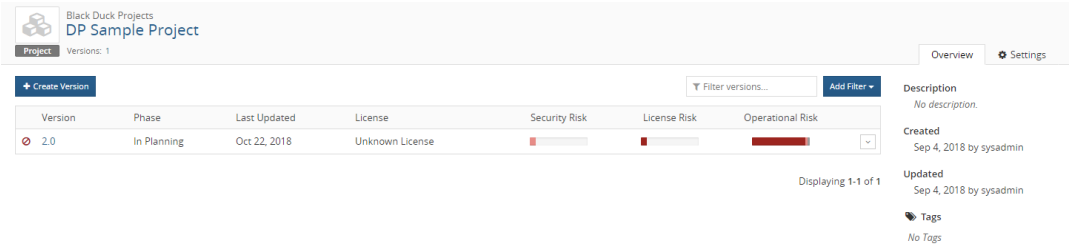
     By default, the user creating the project is the project owner. The owner has the ability to assign their projects to users and groups.

   - Select a tier. [1]

   Note: To assign an application ID to a project, create the project, as described here, and then modify the project settings.

5. Type the version for this project in the **Version** field.
6. Optionally, select **Add version details** to enter additional information such as the planned release date, the project phase, and the method in which the project is being delivered.
7. By default, edits to a version of this project apply to all versions of this project, excluding archived versions and manually added components. Clear this option if you want edits to apply to specific versions only.
8. Click **Create**.

   Black Duck displays the *Project Name* page.



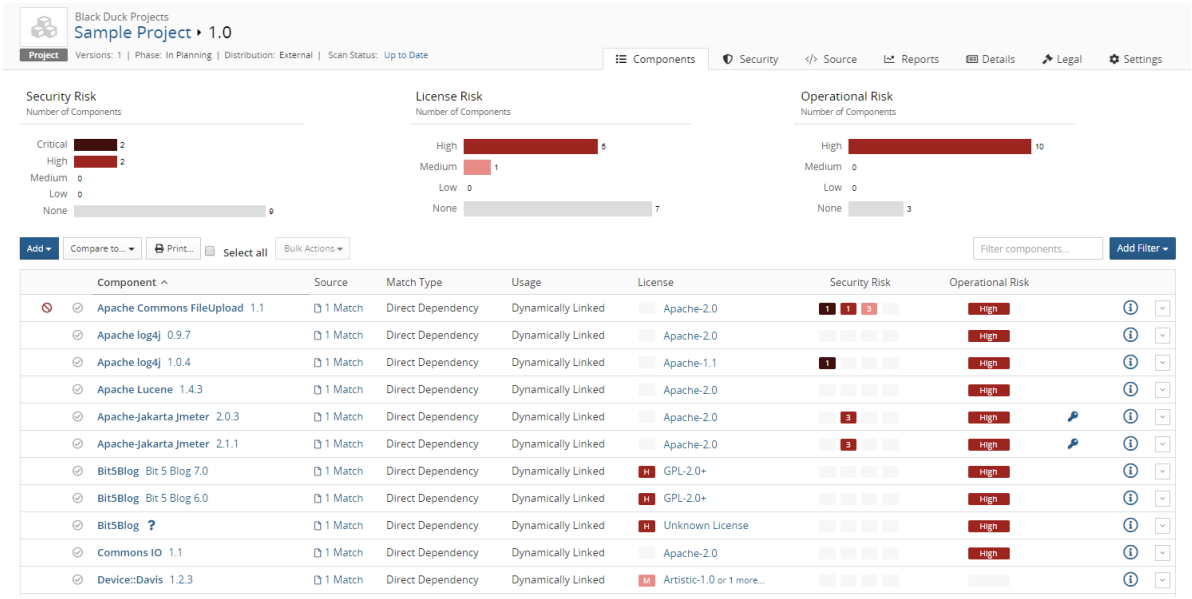
[1] A tier lets you categorize projects in terms of importance to your company. Tier 1 projects are defined as those that are most critical to the company, where Tier 5 projects are defined as least critical.

Once you have mapped a component scan to a project version, the results automatically create the project version's BOM.

To view a project version's BOM

1. Log in to Black Duck.
2. Locate the internal project using the **Projects** tab on the Dashboard.
3. Select the name of the project to go to the *Project Name* page.
4. Select the version name of the project that you want to view.

   The **Components** tab shows you the BOM.



   By default, the BOM displays a "flat" view of components where all components found are listed at the same level. Select **Component Tree** to view a hierarchical view which is based on file system relationships.

Adjusting the component and/or component version in a BOM

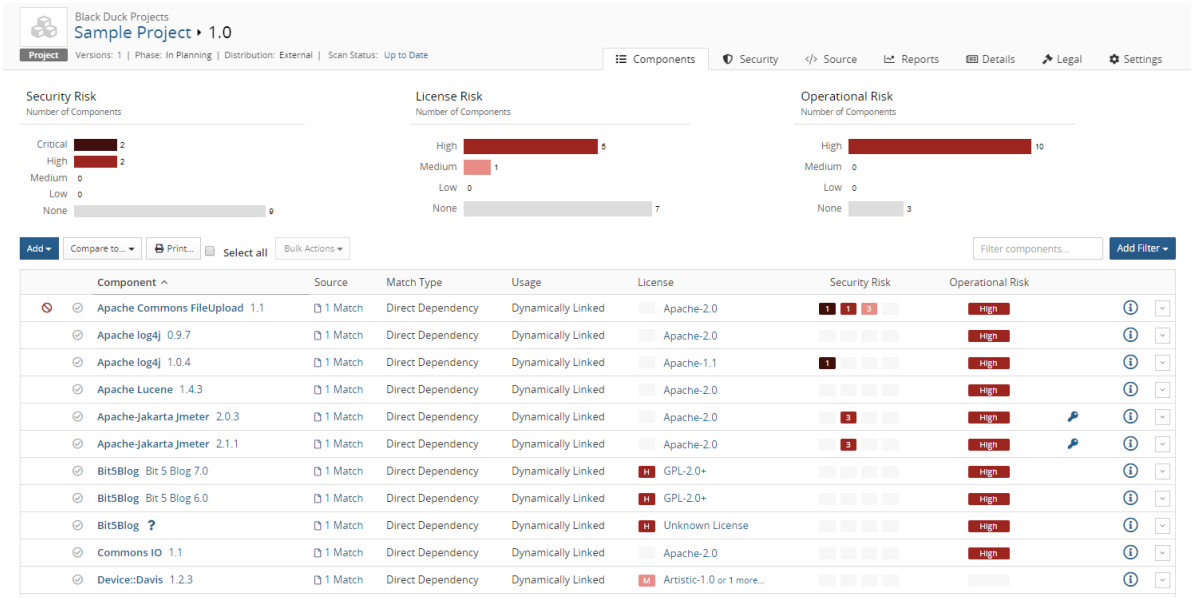
Once you have mapped a component scan to a project version, the scan results automatically create the

project version's BOM. Although component scanning automatically discovers the open source component and component version from most archive files by comparing them to components in the Black Duck KB, you may be using a version of the component that is not available in the Black Duck KB, or you may be using a modified version of a component. You can adjust the component and version for a component in a BOM.

- If the component/version is available in the Black Duck KB, users with the appropriate role can adjust the component or component version, as described below.
- If the component version of a component is not available in the Black Duck KB, users with the Component Manager role can create a custom version and add it to the BOM.

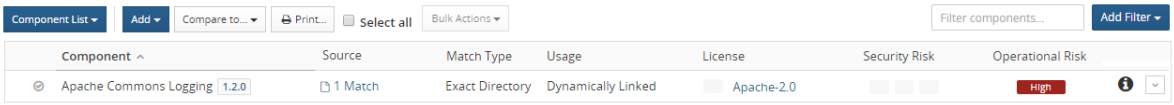
To select an alternate component and/or version match for a component in a BOM

1. Log in to Black Duck.
2. Locate the project using the **Projects** tab on the Dashboard.
3. Select the name of the project to go to the *Project Name* page.
4. Select the version name to open the **Components** tab and view the BOM.



5. In the component list view of the BOM, click and select **Edit** to open the Edit component dialog box.
6. Type the name of the OSS component in the **Component** field and select the alternate match.
7. Select the version of the component from the **Version** list. The list contains all versions of the component that are available in the Black Duck KB.
8. Optionally, enter a purpose for this adjustment and/or select the **Modification** checkbox and optionally, enter information regarding this modification in the field.
9. Click **Save**.

The component and version for the BOM entry are updated. The BOM adjustment indicator ( ) appears in the table row to indicate that the component and/or version were changed from the one automatically discovered in the component scan:

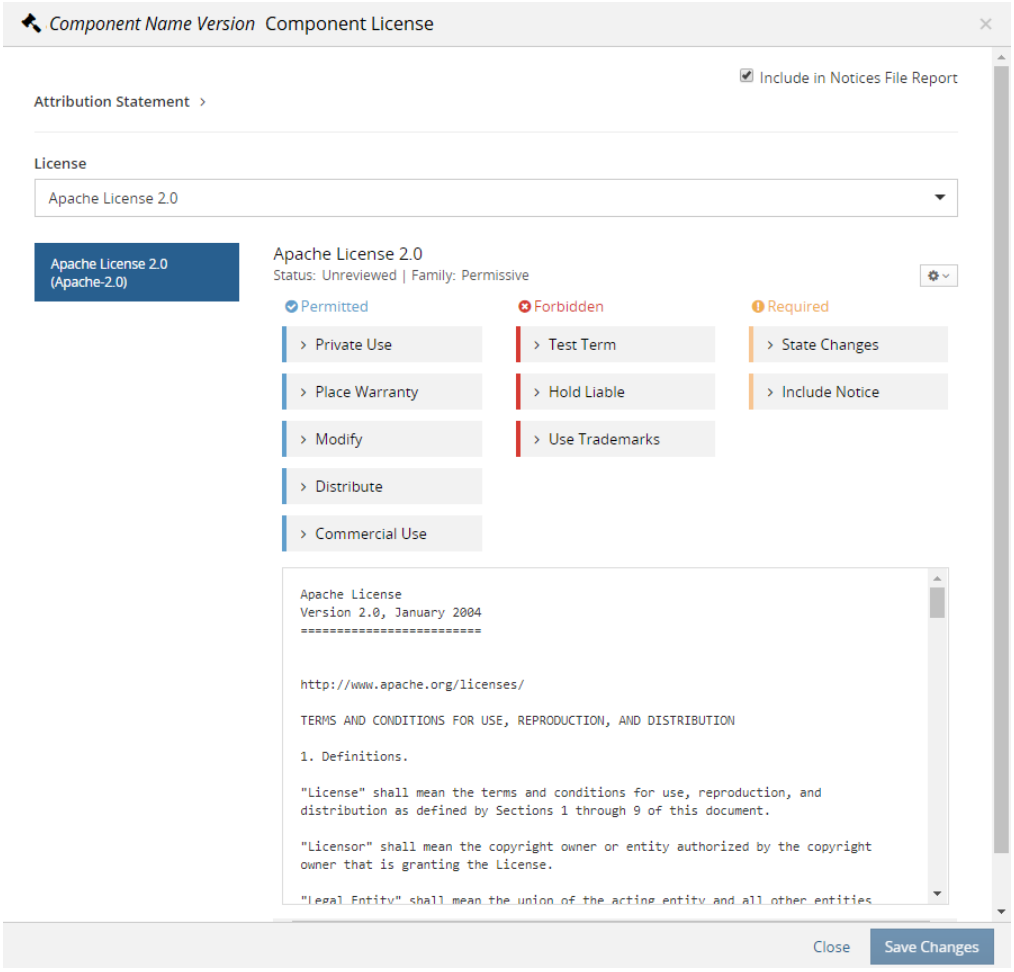


Selecting a different license for a component in a BOM

You can select a license for a component used in a BOM that is different from the component's declared license that is identified in the Black Duck KB.

To select a different license for an OSS component in the project version's BOM

1. Log in to Black Duck.
2. Locate the project using the **Projects** tab on the Dashboard.
3. Select the name of the project to go to the *Project Name* page.
4. Select the version name to open the **Components** tab and view the BOM.
5. Select the existing license to open the *Component Name Version* Component License dialog box.



6. Backspace to clear the field and then type the name of the license that you want to assign, and from the list of suggestions, select the one you want.
7. Click **Save Changes**.

   The assigned license is updated. If the new license carries a different type of license risk than the previous one, the license risk calculations for the component and for the project version are updated. A  appears in the table row to indicate that a manual adjustment was made to this component.

Chapter 4: About security risk

Black Duck helps security and development teams identify security risks across their applications.

By mapping vulnerabilities to your open source software, Black Duck can provide you with high-level overview information on security risk of your projects, along with detailed information on security vulnerabilities which you can use to investigate and remediate your security vulnerabilities.

Vulnerabilities are linked to the open source components by the Common Vulnerabilities and Exposures numbers (CVEs), as reported in the National Vulnerabilities Database (NVD) maintained by the National Institutes of Standards and Technology (NIST) and/or by (BDSA) numbers If you have licensed Black Duck Security Advisories.

Security risk levels

NVD and BDSA use the Common Vulnerability Scoring System (CVSS) which provides a numerical score reflecting the severity of a vulnerability. The numerical score is then translated into a risk level to help you assess and prioritize security vulnerabilities.

Black Duck provides you with the option of viewing CVSS 2.0 or CVSS 3.0 scores. By default, Black Duck displays CVSS 2.0 scores.

- CVSS 2.0 scores has the following values:
  - Low risk: 0.0 - 3.9
  - Medium risk: 4.0 - 6.9
  - High risk: 7.0-10.0

  Note that Black Duck shows vulnerabilities with a 0.0 score as no risk.

  Although CVSS 2.0 does not have a Critical risk category, the security graphs In the Black Duck UI display a Critical risk category. This category will display a value of 0 for CVSS 2.0.

- CVSS 3.0 scores has the following values:
  - None: 0.0
  - Low risk: 0.1 - 3.9
  - Medium risk: 4.0 - 6.9
  - High risk: 7.0 - 8.9
  - Critical risk: 9.0 - 10.0

Suggested work flow

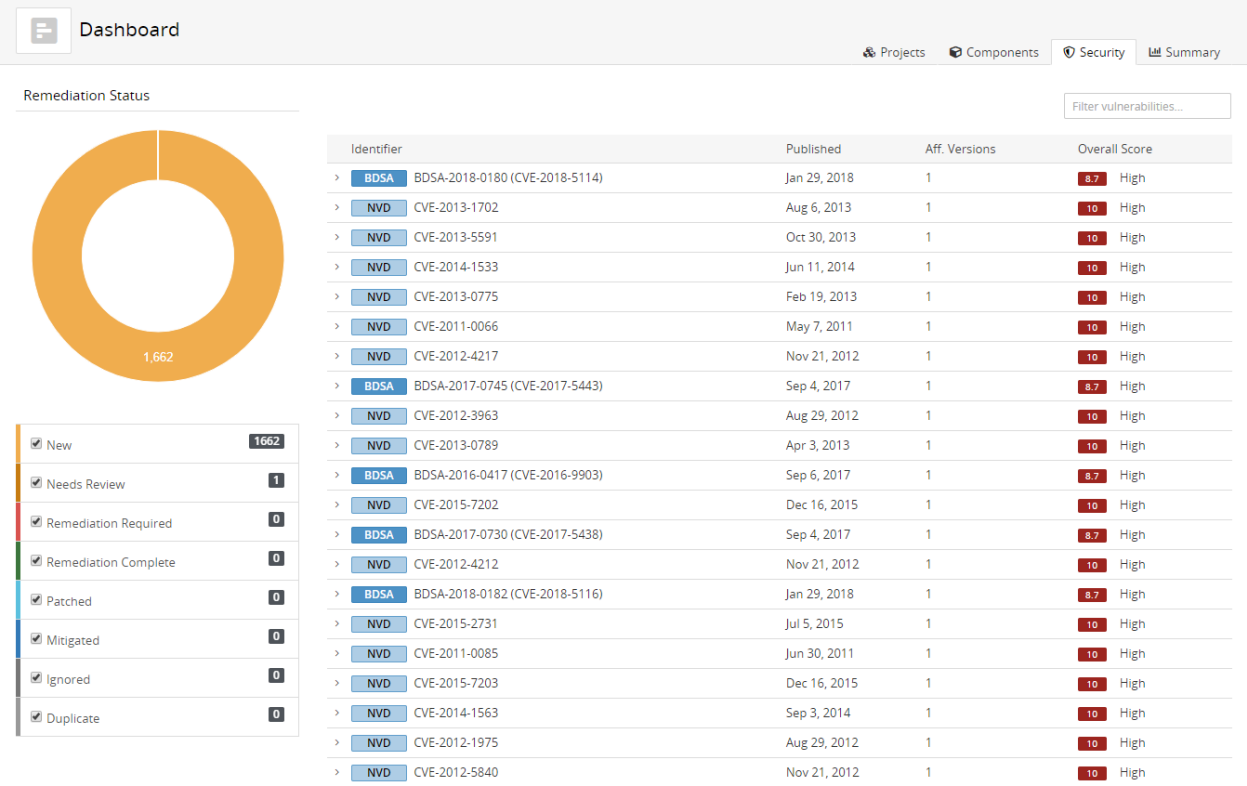
To manage security risk using Black Duck:

1. With the assistance of your security team, determine your security risk policies.
2. If necessary, users with the system administrator role can define the default security risk calculation.
3. Create policies that trigger violations when components do not comply with your security policies.
4. Depending on your interests:
   - Use the Summary Dashboard to view the overall health of your projects and identify areas of concern. Use this page to quickly assess areas where you need to focus your attention.
   - Use these Dashboard pages for a high-level overview information of security risk:
     - Project Dashboard to view the overall security risk across all your projects.
     - Component Dashboard to view the risk for each of the components that are used in one or more of your projects
     - Security Dashboard to view the security risk associated with all the vulnerabilities that exist in your projects. This dashboard also shows the remediation status of all the vulnerabilities that exist within the projects.
   - Use these pages for project version-level information:
     - project version page/**Components** tab, also known as the project version BOM, to view the components specific to that project version, that have security risk.
     - project version page/ **Security** tab to view the security vulnerabilities of each severity associated with the components used in a project version.
5. Investigate vulnerabilities and policy violations. For detailed information on security vulnerabilities, view the:
   - CVE page
   - BDSA page if you have licensed Black Duck Security Advisories (BDSA)
6. After reviewing the severity of the vulnerability, users with the appropriate role can change the remediation status of the security vulnerability.
7. Monitor notifications for any new security vulnerabilities.

   You will receive notification alerts if security vulnerabilities are published or updated against components that are included in one or more of your projects.

Viewing all security vulnerabilities

Use the Security Dashboard to identify and manage risk. This dashboard lists all the security vulnerabilities that affect your projects.



Using the Security Dashboard is an efficient way to:

- Identify the remediation status of all the vulnerabilities in your projects.
- Review the severity of the vulnerability to determine if remediation is required.

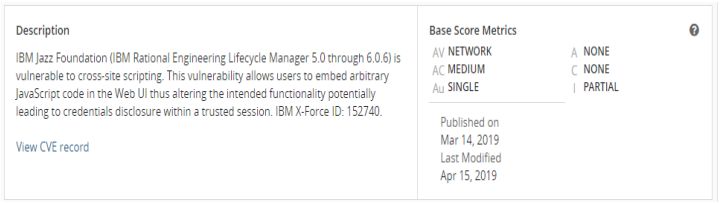
Note: The security risk values shown use CVSS 2.0 or CVSS 3.0 scores, depending on which security risk calculation you selected; by default CVSS 2.0 scores are shown.

To use the Security Dashboard to identify and manage risk

1. Log in to Black Duck.
2. From the Dashboard, click the **Security** tab to display the Security Dashboard.
3. You can use:
   - The table filter field to filter the vulnerabilities shown in the table by identifier.
   - The **Aff. Versions** column to view the number of project versions affected by this vulnerability. Use this column to identify the vulnerabilities that are affecting the greatest number of versions of your projects.
   - The Remediation Status chart to view the remediation status of all vulnerabilities that exist within all projects and the number of vulnerabilities with each remediation status.

     By default, the chart displays all remediation statuses. Clear the check box to hide the vulnerabilities with that remediation status.

- The **Overall Score** column shows the Temporal score (for BDSA), or Base score (for NVD) and associated risk level. Hover over the **Overall Score** value to see the individual values.
  - For BDSA, the Temporal, Base, Exploitability, and Impact scores are shown.
  - For NVD, the Base, Exploitability, and Impact scores are shown.
- The table to view more information on a vulnerability by selecting **>** next to the vulnerability that interests you.



Select to view the BDSA record and/or the CVE record from which you can remediate the vulnerability, if you have the appropriate role.

Note: A single vulnerability can be present multiple times in the remediation status pie chart since it can have multiple different remediation types within a single BOM or across multiple project version BOMs. However, a single vulnerability is listed in only one row in the table.

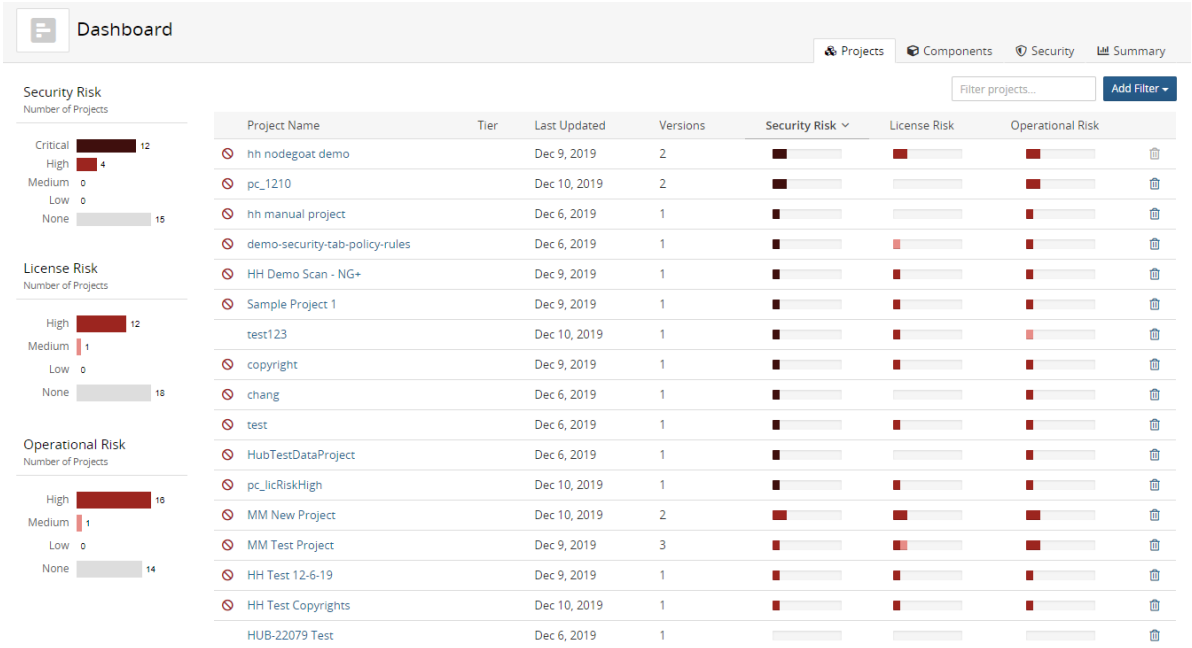
Viewing the security vulnerabilities of your projects and project versions

Use the Project Dashboard to view the types and severity of risk that are associated with the components that are in one or more versions of your projects. This dashboard provides an overall view of risk across all of your projects.

Note that the security risk values shown use CVSS 2.0 or CVSS 3.0 scores, depending on which security risk calculation you selected; by default, CVSS 2.0 scores are shown.

To view the security vulnerabilities

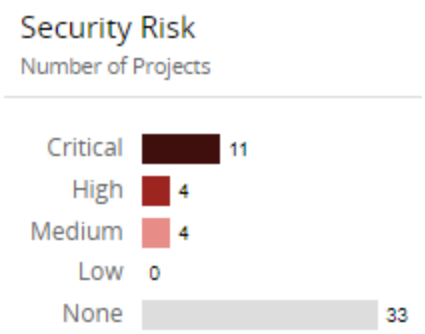
1. Log in to Black Duck.
2. From the Dashboard, select the **Projects** tab to display the Project Dashboard.



Tip: You can also click the logo in the upper left corner of the navigation bar to view the Project Dashboard.

From this page:

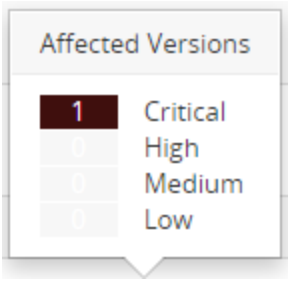
- Use the Security Risk graph to view the number of projects that for each risk category.



Select one or more values in the graph or use the filters at the top of the table to view the projects that have one or more security risk levels. Note that the graph displays a Critical risk category with a value of 0, if you selected CVSS 2.0.

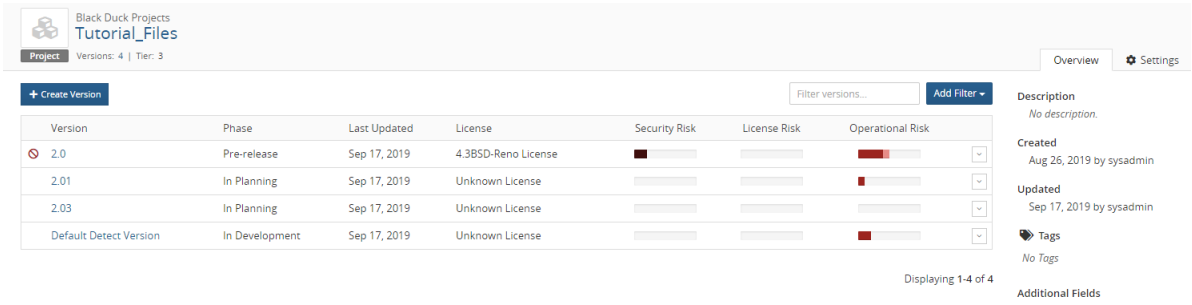
Note: The Security Risk graph displays the highest security risk level for a project, not all security levels affecting a project. Select a project name to open a page which lists all security risk levels for all versions of that project.

- Select a bar in **Security Risk** column in the table to see the number of versions of this project that are affected by a security risk.

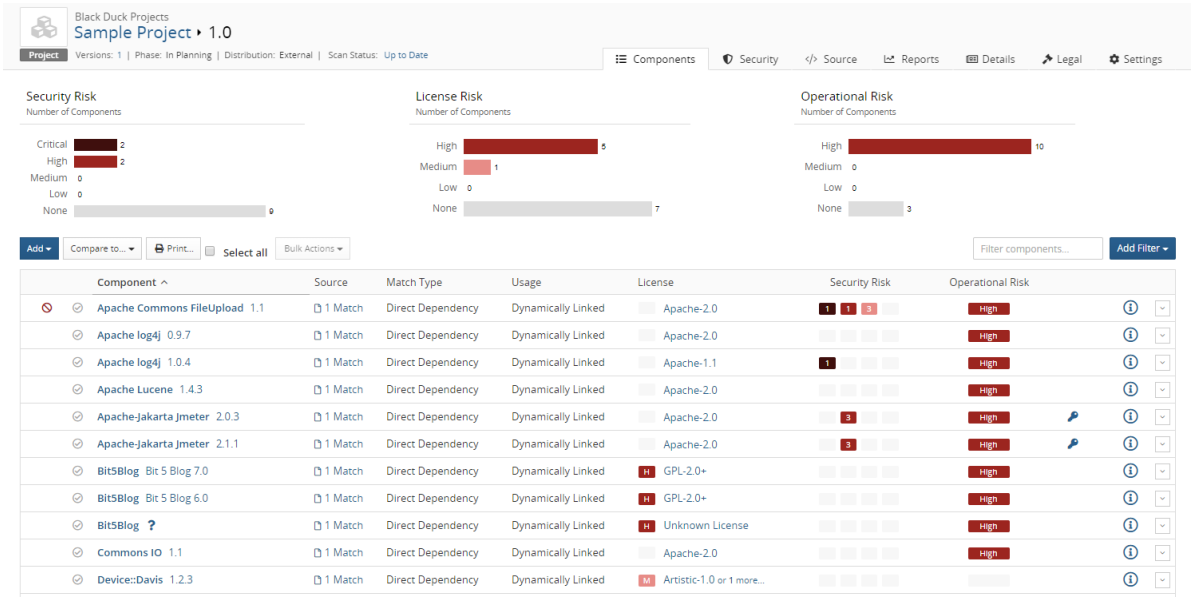


Use this column to identify the vulnerabilities that are affecting the greatest number of your projects.

3. Select a project name to view a page that lists all versions of this project.



4. Select a version with security risks to view a page which shows the BOM for this version of the project.



5. Use this page to view more information on the component and component version.

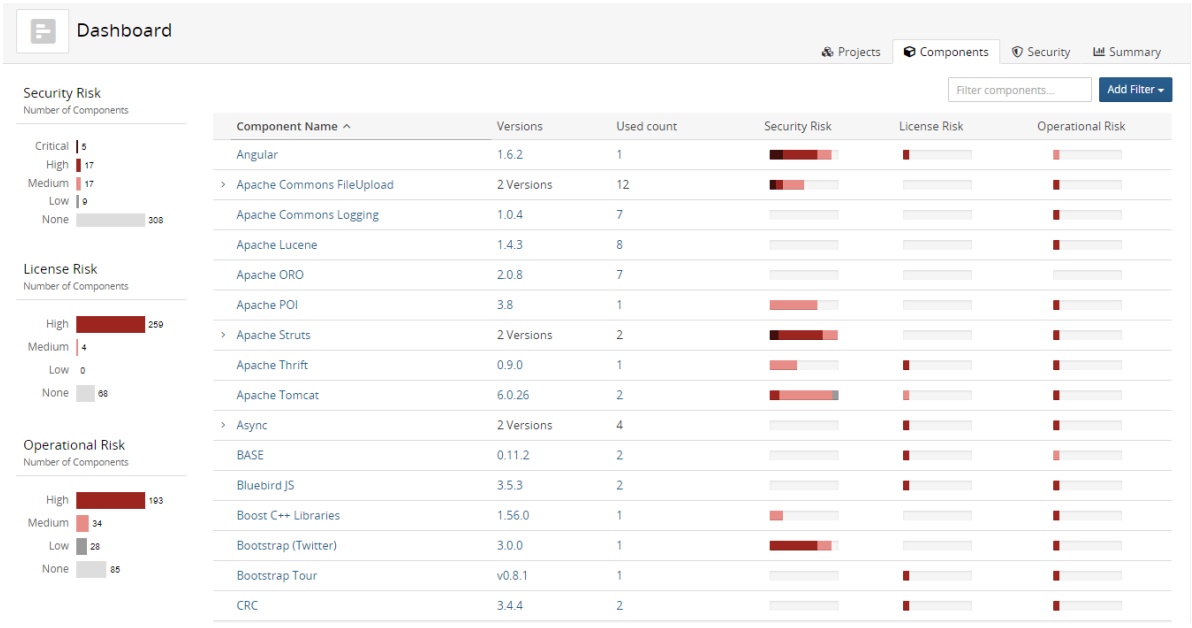
Viewing security vulnerabilities associated with your components

Use the Component Dashboard to view all components in your projects; components shown are top-level (parent) and subcomponents. The table lists the components used in one or more of your projects. On the left side of the page risk graphs show the total number of components used in one or more of your projects, which have each severity of security, license, and operational risks associated with them. From this page, you can drill down and view more information on these components and their vulnerabilities.

Note that the security risk values shown use CVSS 2.0 or CVSS 3.0 scores, depending on which security risk calculation you selected; by default, CVSS 2.0 scores are shown.

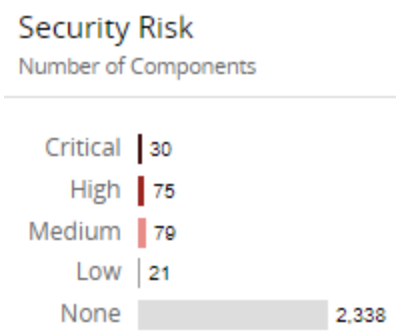
To view vulnerabilities of components in your projects

1. Log in to Black Duck.
2. Select the **Components** tab to display the Component Dashboard.



From this page:

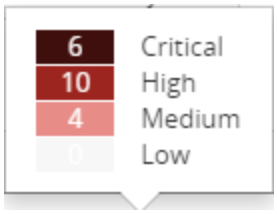
- Use the **Security Risk** graph to view the total number of components, used in one or more of your projects, for each level of security risk.



Select a value in the **Security Risk** graph to view the components that have that security risk level. Note that the graph displays a Critical risk category with a value of 0, if you selected CVSS 2.0.

Note: This graph lists the number of components which have this level of security risk as their *highest* risk level – it is not the total number of components which have this risk level. For example, if you select to view components with a medium risk level, only those components that have medium as the highest risk level appear in the table; components that have both high *and* medium vulnerabilities are not shown.

- Select a bar in **Security Risk** column in the table to identify the components that have the greatest number of vulnerabilities.

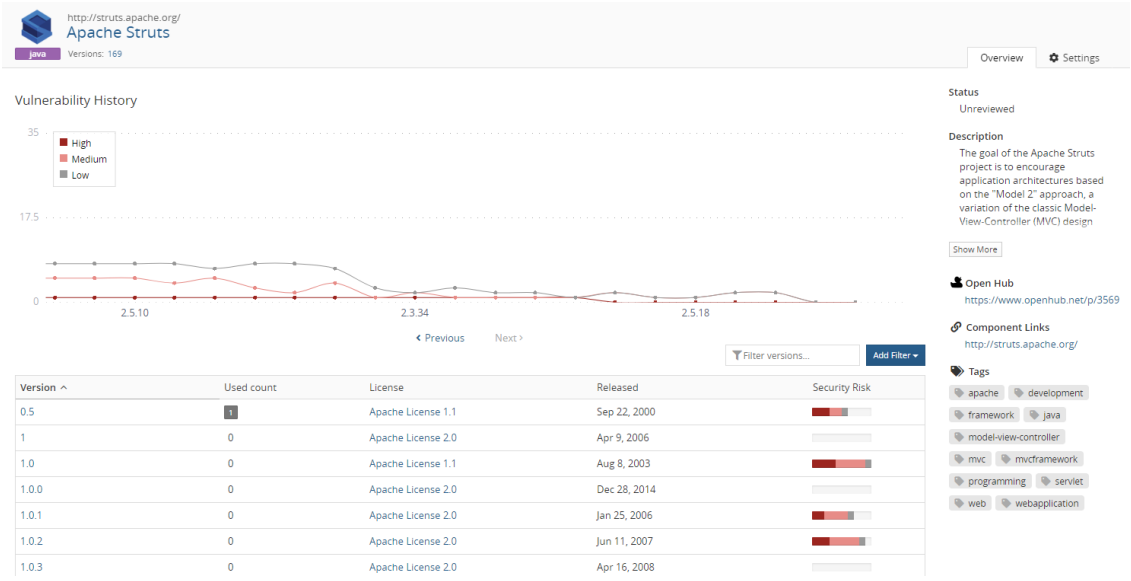


For each version of a component, the values for each risk level are calculated as:

```
# of vulnerabilities * the number of files affected by the
vulnerability for each version of the project
```

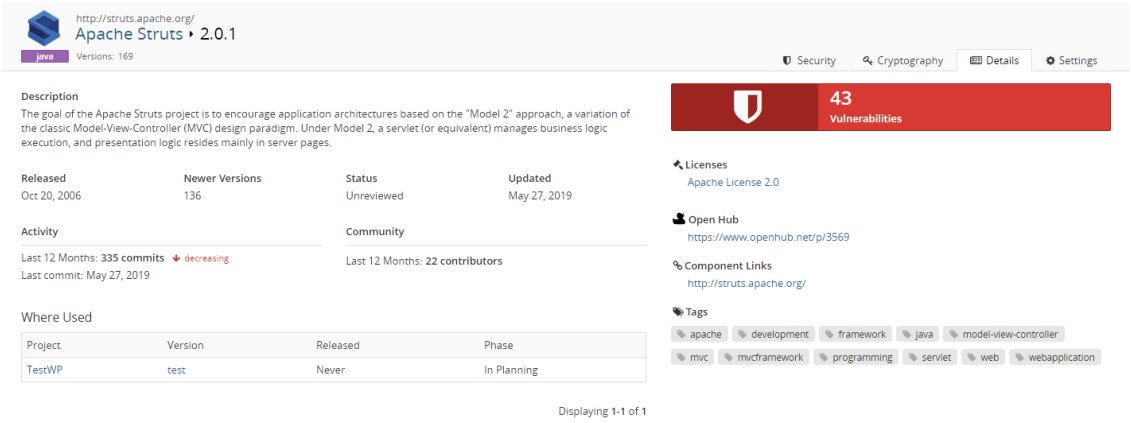
For components that have multiple versions, the total value equals the sum of all versions.

3. Click **>** for components with multiple versions to view a list of the versions used in your projects.
4. Optionally, to view the vulnerabilities for a specific version of a component:
   - Select a component name. The **Overview** tab lists all versions of this component, along with a description:

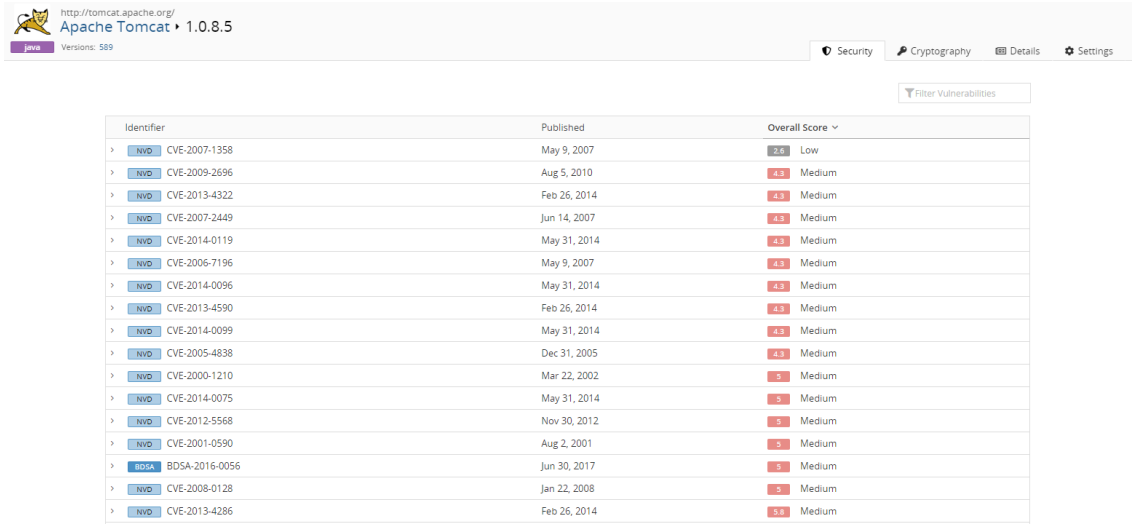


The **Used count** column shows the number of project versions that use this version of this component. A graph at the top of the page shows a history of high, medium, and low vulnerabilities for each version of this component.

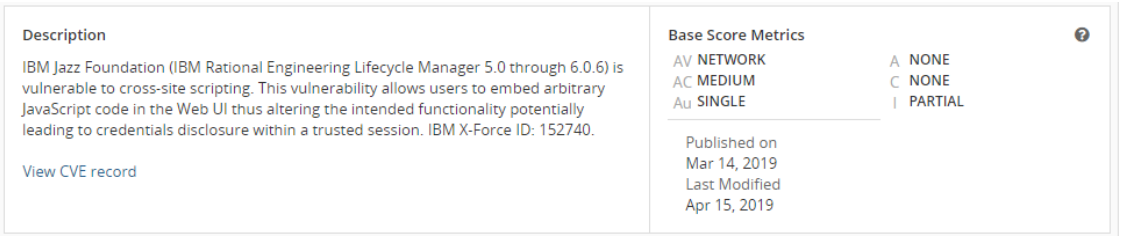
- Select a component version to view a page which lists all projects and associated versions that use this version of this component. The number of vulnerabilities, a brief description, and associated licenses with this project also appear on this page.



Click the **Security** tab to view a list of the vulnerabilities for this version of the component.



Click **>** to view more information on a vulnerability.

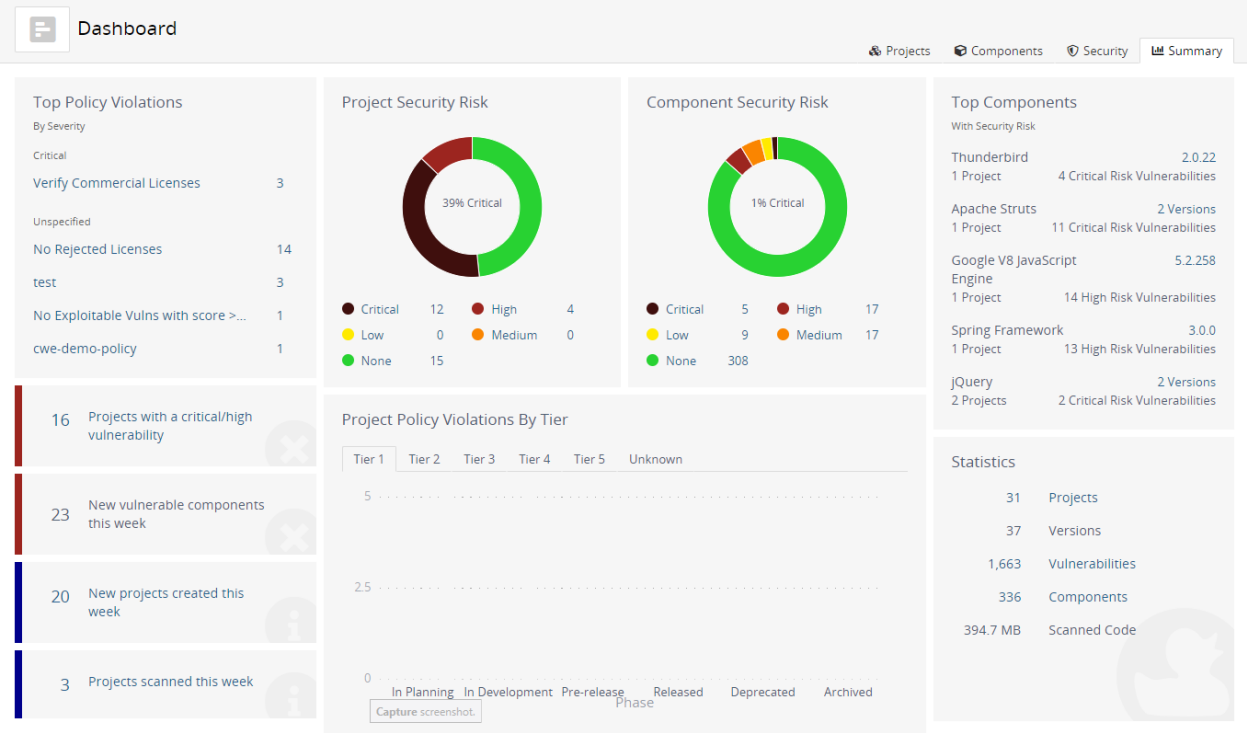


Note: The Authentication value is not available for CVSS 3.0 scores.

Select the link shown to view the CVE record or BDSA record (if you licensed BDSA).

Viewing the health of your projects

Use the **Summary** tab to view the overall health of your projects and identify areas of concern. The page consists of widgets that provide business critical information which you can use to quickly assess areas where you need to focus your attention.



Note: The **Summary** tab only displays information for the projects you have permission to view.

The following table describes each widget shown on the **Summary** tab and, where available, how to view additional information. Note that the security risk values shown use CVSS 2.0 or CVSS 3.0 scores, depending on which security risk calculation you selected; by default CVSS 2.0 scores are shown. Note that the graphs display a Critical risk category with a value of 0, if you selected CVSS 2.0.

Description	More Information
The **Top Policy Violations** widget displays up to the top five policy violations across all projects that you have permission to view. Policy rules are listed by severity level and then by the number of policy violations, in descending order. If policy rules do not have severity levels assigned to them, the widget displays the top five policy violations, in descending order by the number of violations. • If you do not have the Policy Management module, this widget will not appear on the page. • A message appears if you have the Policy Management module but do not have any policy rules configured or have any policy violations.	Select a policy rule to view the **Projects** tab filtered to display the projects with a version that violate that policy rule.
The **Project Security Risk** widget displays the number of projects you have permission to view for each level of security risk. Note that this widget counts the highest security risk level for a project, not all security levels affecting a project. For example, if a project has medium and low security risks, it is counted as a project with medium security risk; it is not included as a project with low security risks.	Hover over the graph to view the number of projects with that level of security risk.
The **Component Security Risk** widget displays the number of components in projects you have permission to view for each security risk level. Note that the widget counts only the highest security risk for a component. For example, if a component has medium and low security risks, it is counted as one component with a medium security risk.	Hover over the graph to view the number of components with that level of security risk.
The **Top Components with Security Risk** widget displays up to the top five components used in the projects you have permission to view. The information shown for each component is: • Component name and number of versions used in your projects. If only one version is used, the specific version is listed here. • Number of your projects that have this component. • Number of security risks in this component, with the highest security risk listed here. Components are organized by security risk, with those components with the highest risk listed first.	Select the number of versions link to view the Component Dashboard page. Select the specific version to view the Component Version Details page.
The **Projects have a critical/high vulnerability** widget displays the number of projects with versions that contain components with a critical and/or high security risk.	Select the text to view the **Projects** tab filters to show the projects that have versions that have critical and/or high security risk.

Description	More Information
The **New vulnerable components this week** widget displays the number of components the Black Duck KB mapped a vulnerability to in the past seven days, including today.	N/A.
The **New projects created this week** widget displays the number of projects that you have permission to view that have been created in the past seven days, including today.	Select the text to view the **Projects** tab which lists the projects created in the past week.
The **Projects scanned this week** widget displays the number of projects with scans from the past seven days, including today.	Select the text to view the **Projects** tab showing projects that have project versions with scans from the past week.
The **Project Policy Violations by Tier** widget displays the total number of projects by phase that have a policy violation, grouped by tiers. • If you do not use tiers for your projects, projects are grouped in a single category called **Unknown**. • If you do not have the Policy Management module, this widget displays **Projects by Tier**.	For each tier, hover over a bar to see the number of projects in this phase and the number of projects in this phase with a policy violation.
The **Statistics** widget displays the following information: • **Projects** lists the number of your projects. • **Versions** lists the number of project versions for your projects. • **Vulnerabilities** lists the number of vulnerabilities in your projects. • **Components** lists the number of components used in your projects, *including* ignored components. • **Scanned Code** lists the number of GBs scanned for all scans.	Select the projects value to view the **Projects** tab listing all projects you can view. Select the vulnerability value to view the **Security** tab filtered to show the vulnerabilities with a New, Needs Review, or Remediation Required status. Select the components value to view the **Components** tab showing all components used in the projects you can view. Note that this tab *excludes* ignored components.