sonatype

# Guide to the Nexus Vulnerability Scanner

## Instantly generate an inventory of your open source and third party components to determine potential security and license risk.

Gain visibility into the open source components used in an application and discover potential security, licensing, and quality problems. The Nexus Vulnerability Report evaluates your internal and third party applications for potential vulnerabilities and provides guidance for how to resolve.

- Confidentially and quickly analyze your open source and third party components.
- Create a precise “bill of materials” to identify which open source components are used and where.
- Discover all component dependencies and known vulnerabilities or license risks.
- Identify known cyber vulnerabilities that may impact software security.
- Discover potential component quality concerns – such as restrictive GPL licenses and age.
- Ideal for Cyber Supply Chain Act initiatives, GDPR, and other regulatory or compliance mandates.

Sample Report

### Scope of Analysis

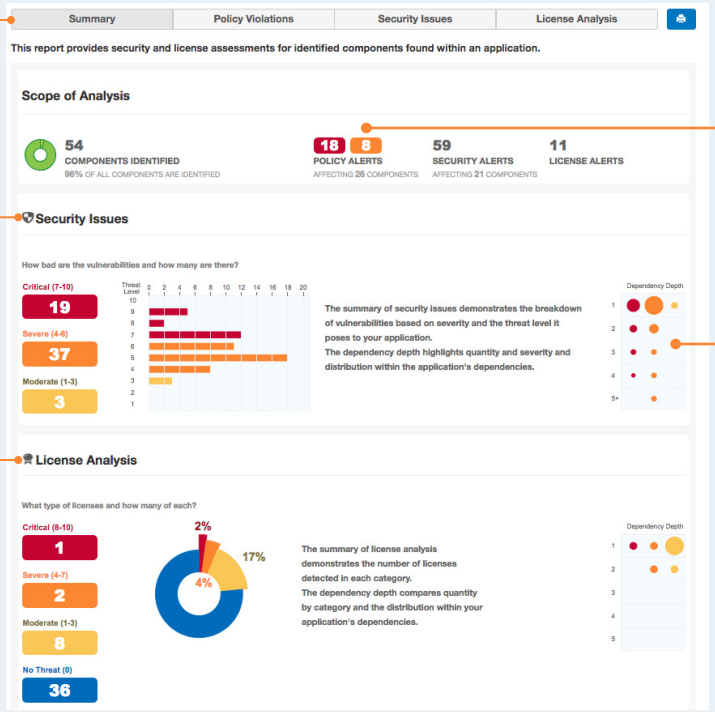
High level summary of the number of components we found, as well as the number and severity of policy, security and license alerts. The full, detailed report lists each alert in detail.

### Security Issues

This section identifies the breakdown of vulnerabilities based on severity and the threat level it poses to your application. Severity levels are based on CVSS ratings.

### License Analysis

This section defines the number of licenses detected in each category, including risk classifications.




### Policy Alerts

Policy violations shown in this report are based on pre-set, standard policy definitions established by Sonatype. Nexus Lifecycle customers are able to customize their policies.

### Dependency Depth

This chart shows how deep within the dependency tree your issues are located.

# Policy Violations

### Policy Violations

The Policy tab displays a list of all components found during scan of application. By default, components are ordered by their worst policy violation. This is an important distinction, because a component may have more than one violation, and the threat level severity for those violations could vary.

### Filter

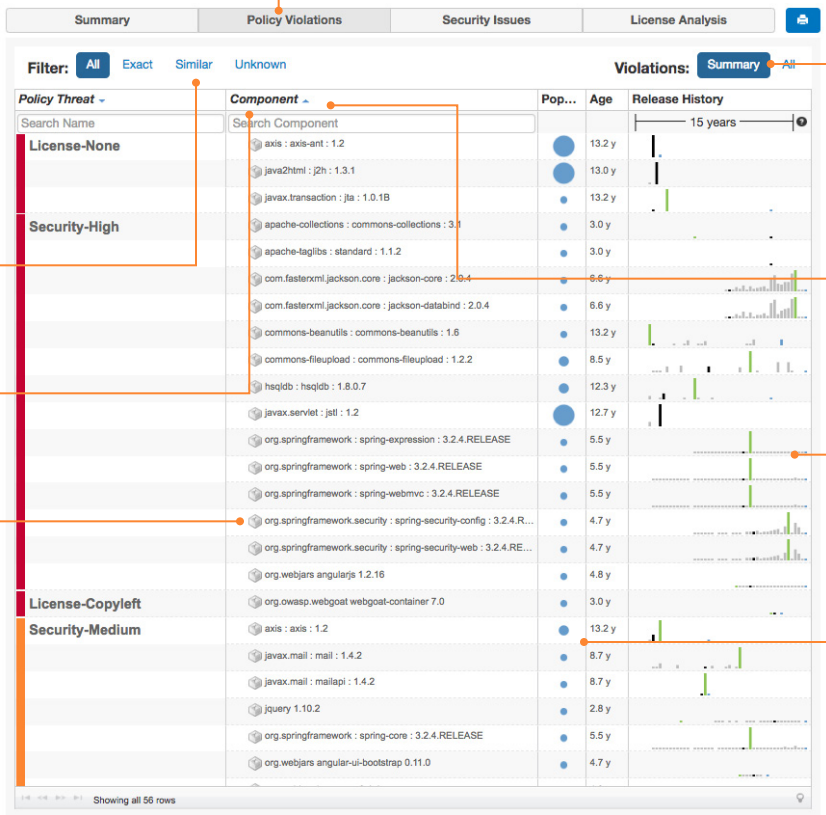
Use the filter to display components by their match type.

### Sort

Click columns to sort.

### Component Bill of Materials

This lists the specific components found in an application, also known as an application “bill of materials.”




### Summary

Some components may violate more than one policy. Summary only shows the violation with the highest threat. Use “All” to see every violation associated with each component.

### Coordinates

This column contains the Maven coordinates for the components found in your evaluation.

### Release History

Shows where your component (the black bar) falls within the most popular (green bar) and most recent release (blue bar).

### Popularity

Represents the relative popularity of the component you are using. Larger circles indicate which version of the component is more popular.

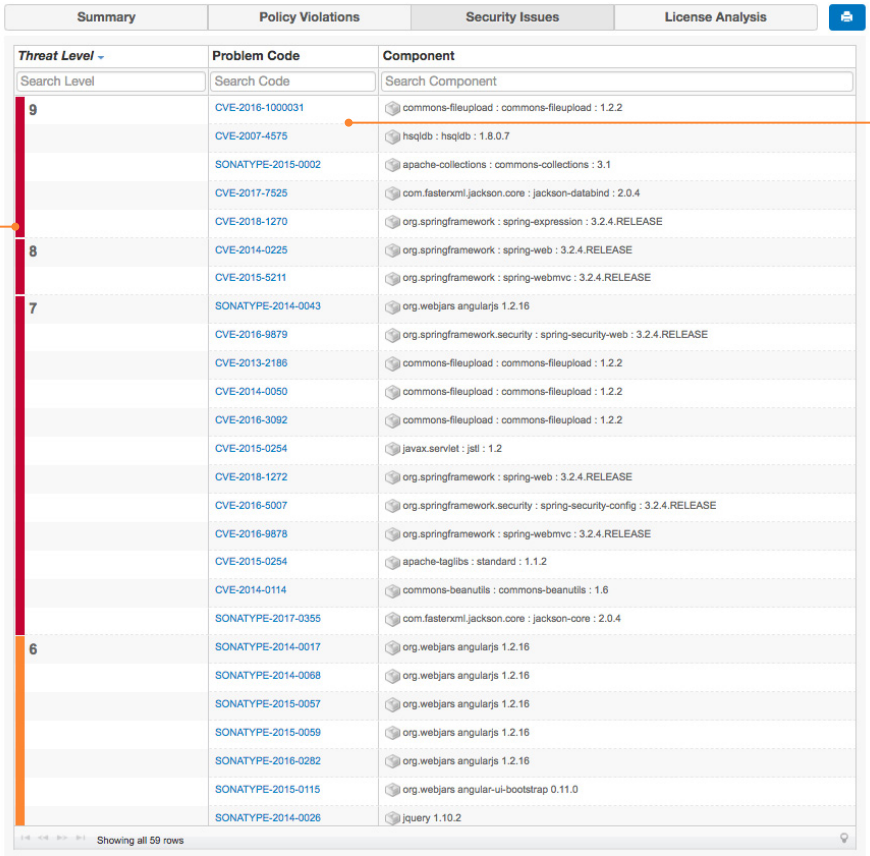
**To generate a Nexus Vulnerability Report, please go to sonatype.com/appscan**

# Security Issues

Review and investigate any security vulnerabilities found in the component in your application.

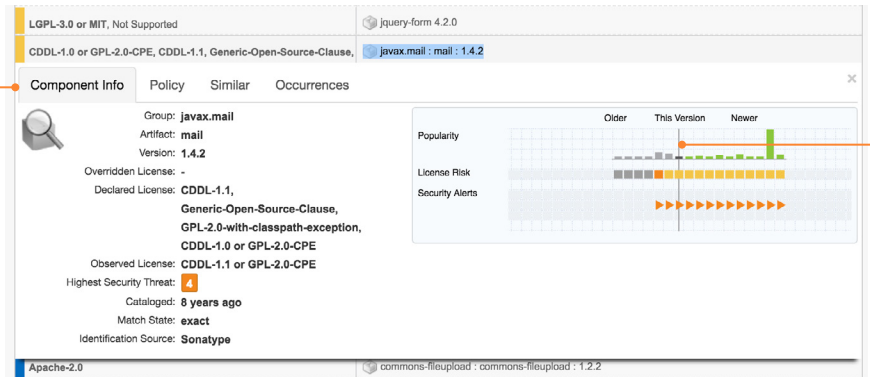
### Threat Level

Security threat levels shown in this area do not correspond to policy, but rather the Common Vulnerability Scoring System (CVSS) score.




### Component Info

Click on any specific component listed in any page of your report to see deeper detail.




### Problem Code

Go directly to the source to drill down on the details for any vulnerability.

### Version Slider

In this Component Detail screen, compare the security and license risk of your current component version to newer versions. Move the slider to see the newer component version numbers and details.

**To generate a Nexus Vulnerability Report, please go to sonatype.com/appscan**

# License Analysis

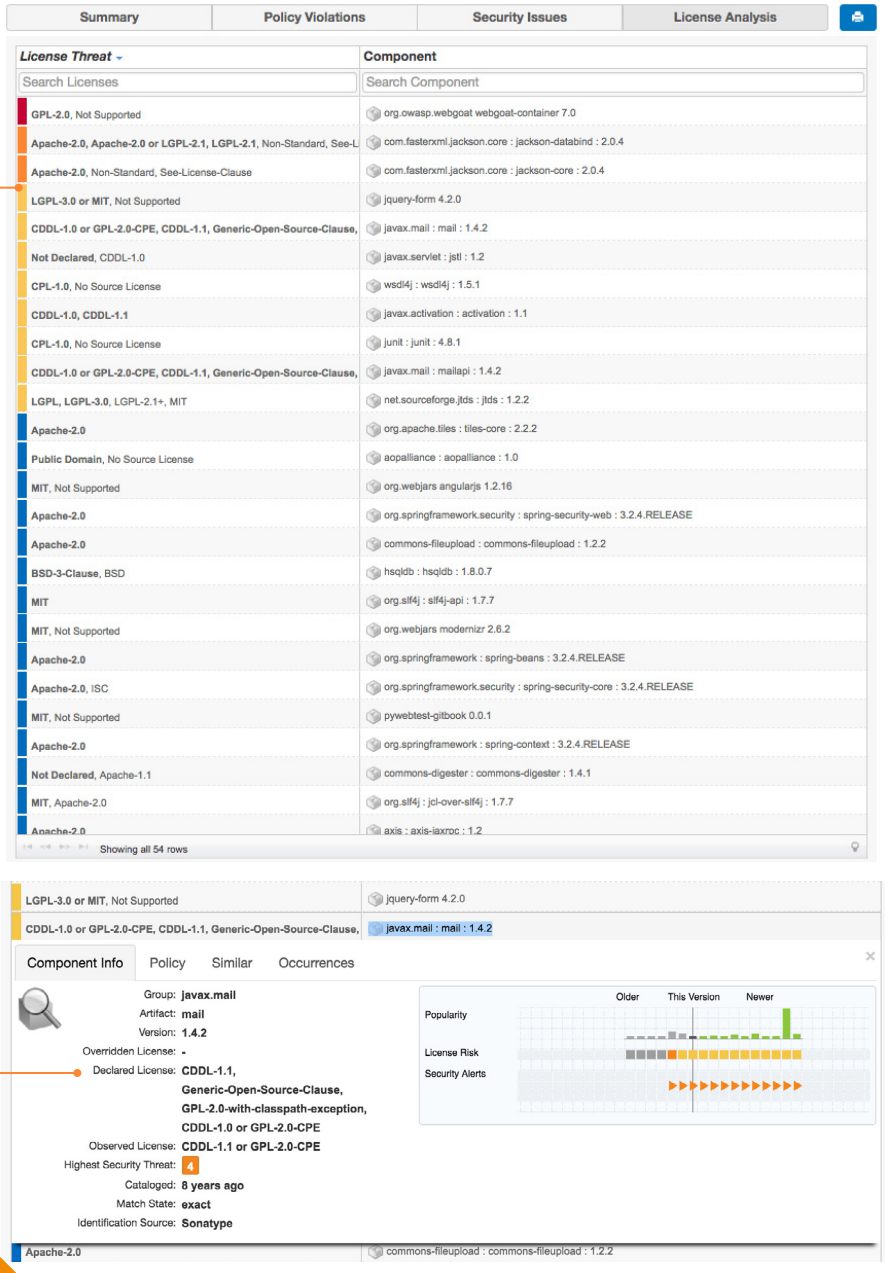
Review and investigate license information for every component in your application.

### License Threat

Licenses are sorted by threat level with the riskiest at the top. Licenses are categorized as Copyleft (red), Non-standard or Not Provided (orange), Weak Copyleft (yellow) and Liberal (blue).

### Details

Drill down to see details about any component license, including information about declared or observed licenses, and whether a newer component version exists.




### Scanning

We scan the source code looking for license declarations, and determine if the declared license is correct or if there is still hidden risk.

**To generate a Nexus Vulnerability Report, please go to sonatype.com/appscan**

# What's next after your Vulnerability Scan?

Seeing your first Nexus Vulnerability Report can lead to more questions, such as "What can I do about this?" or "Where do I start?" We've helped thousands of organizations answer those questions.

## Nexus Firewall: Block undesirable components from entering your software supply chain.

Nexus Repository Manager is an important first step toward improving the overall quality of your component sourcing, sharing, storage and deployment process. When you augment your repository with Nexus Firewall, you can establish policies to block undesirable binaries from entering the repository and being released to staging.

## Nexus Lifecycle: Automate open source governance across your entire SDLC.

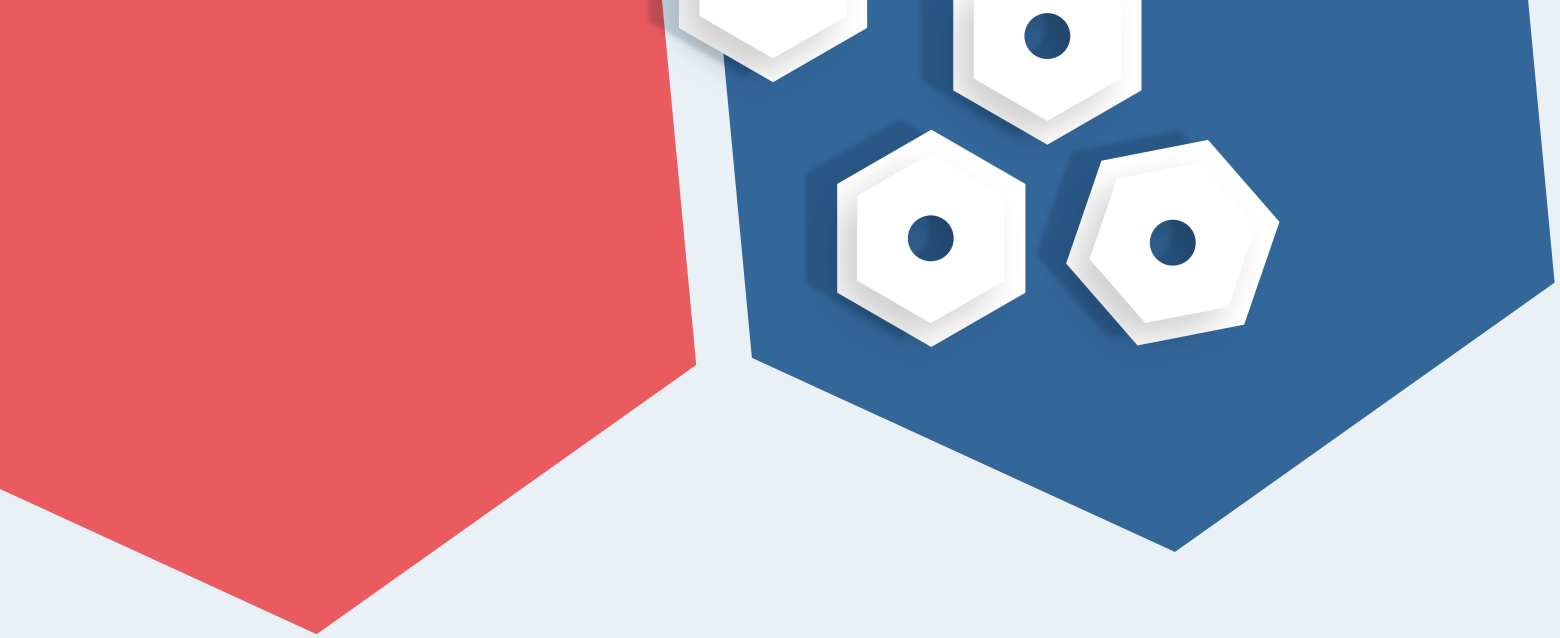
Your free report gives you enough information to start remediation in your application(s) right away, however the goal is to keep undesirable components out of your software to minimize the impact of un- planned work on your development teams and ensure your applications are secure.

With Nexus lifecycle, you can define and enforce open source policies at any point in your software development life cycle.

## Nexus Auditor: Advanced, continuous monitoring of your production applications.

Nexus Auditor allows you to define policies and evaluate the quality of components used within production applications. Understand your risk exposure for third party applications or apps no longer being actively developed with customizable dashboards.

**For more information, please visit**
www.sonatype.com/get-nexus-sonatype



sonatype

More than 10 million software developers rely on Sonatype to innovate faster while mitigating security risks inherent in open source. Sonatype's Nexus platform combines in-depth component intelligence with real-time remediation guidance to automate and scale open source governance across every stage of the modern DevOps pipeline. Sonatype is privately held with investments from TPG, Goldman Sachs, Accel Partners, and Hummer Winblad Venture Partners. Learn more at www.sonatype.com.

**Headquarters**
8161 Maple Lawn Blvd, Suite 250
Fulton, MD 20759
United States – 1.877.866.2836

**European Office**
1 Primrose Street
London EC2A 2EX
United Kingdom

**APAC Office**
5 Martin Place, Level 14
Sydney 2000, NSW
Australia

**Sonatype Inc.**
www.sonatype.com