



# Accelerate Innovation with Automated Security

Enforce Open Source Policies with the Nexus Platform

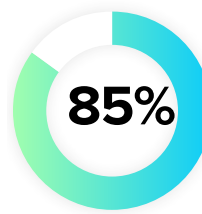
# It's no secret... developers use open source software.

Still, there are questions around how it should be managed—and for good reason. Here's why:

- ▶ Open source components are not created equal. Some are vulnerable from the start, while others go bad over time.
- ▶ Usage has become more complex. With tens of billions of downloads, it's increasingly difficult to manage libraries and direct dependencies.
- ▶ Transitive dependencies: if you are using dependency management tools like Maven (Java), Bower (JavaScript), Bundler (Ruby), etc., then you are automatically pulling in third party dependencies—a liability that you can't afford.

## How do you manage open source risk at scale?

Through an automated open source governance policy.



of most modern applications are comprised of open source components.



**300,000+**

open source components are downloaded annually by the average company.



**500 billion**

download requests of Java, npm, PyPi, and RubyGems were recorded in 2018.

## DevSecOps: Why is open source policy critical?

As the number of breaches continue to rise, DevOps organizations are making investments to better protect themselves by doing more than just building stronger castle walls. These organizations are taking steps to integrate and automate security across the development lifecycle to build quality into their software.

According to the 2019 DevSecOps Community Survey:

**1 in 10**

open source component downloads contain a known security vulnerability.



**71%**

increase in verified or suspected breaches between 2014 and 2019.



**1 in 4**

organizations experienced at least one open source breach in the last 12 months.

**38%**

of organizations have no open source governance policy or ignore it.



# Accelerate DevSecOps early, everywhere, at scale with the Nexus platform.



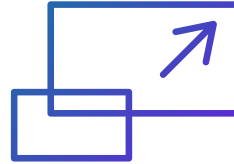
## Early

Nexus delivers intelligence within existing developer workflows and vetted components can be automatically quarantined based on policy.



## Everywhere

Nexus accelerates DevOps by integrating with the most widely used tools at every stage of the development pipeline.



## At Scale

Automate security in a DevOps pipeline with precise component intelligence.

“Integrating security into DevOps to deliver “DevSecOps” requires changing mindsets, processes and technology. Security and risk management leaders must adhere to the collaborative, agile nature of DevOps to be seamless and transparent in the development process, making the Sec in DevSecOps silent.”

**Gartner**

## But first, our data.

Our data quality is the lifeblood that powers our entire platform.

### 97% of Nexus Intelligence is exclusive to Sonatype.

The bulk of our data is collected from verified online advisories and our in-house team of 65 security researchers. In fact, Sonatype’s team has uniquely discovered 1.4 million vulnerable component versions, providing more data than just what’s in the National Vulnerability Database.

### No false positives and no false negatives.

Through both automation and careful human curation, Nexus Intelligence is designed to give you results you can count on, saving you an average of \$14,000 in time per developer per year.

### When it comes to security, speed matters.

We implement a 12-hour fast track for critical and time-sensitive vulnerabilities. You’ll experience a **20% reduction in probability** of a breach when using the Nexus platform.

“The reason **we picked Lifecycle over the other products** is, while the other products were flagging stuff too, they were flagging things that were incorrect.”

— E. KWAN (FINANCIAL SERVICES), IT CENTRAL STATION REVIEW

# Better together.

The Nexus Platform protects your entire software development lifecycle.



## nexus firewall

Vet parts early and automatically stop defective components from entering your DevOps pipeline.



## nexus lifecycle

Empower teams with precise component intelligence that enforces policy and continuously eliminates risk.



## nexus repository

Manage libraries and store parts in a universal repository and share them across the DevOps pipeline.

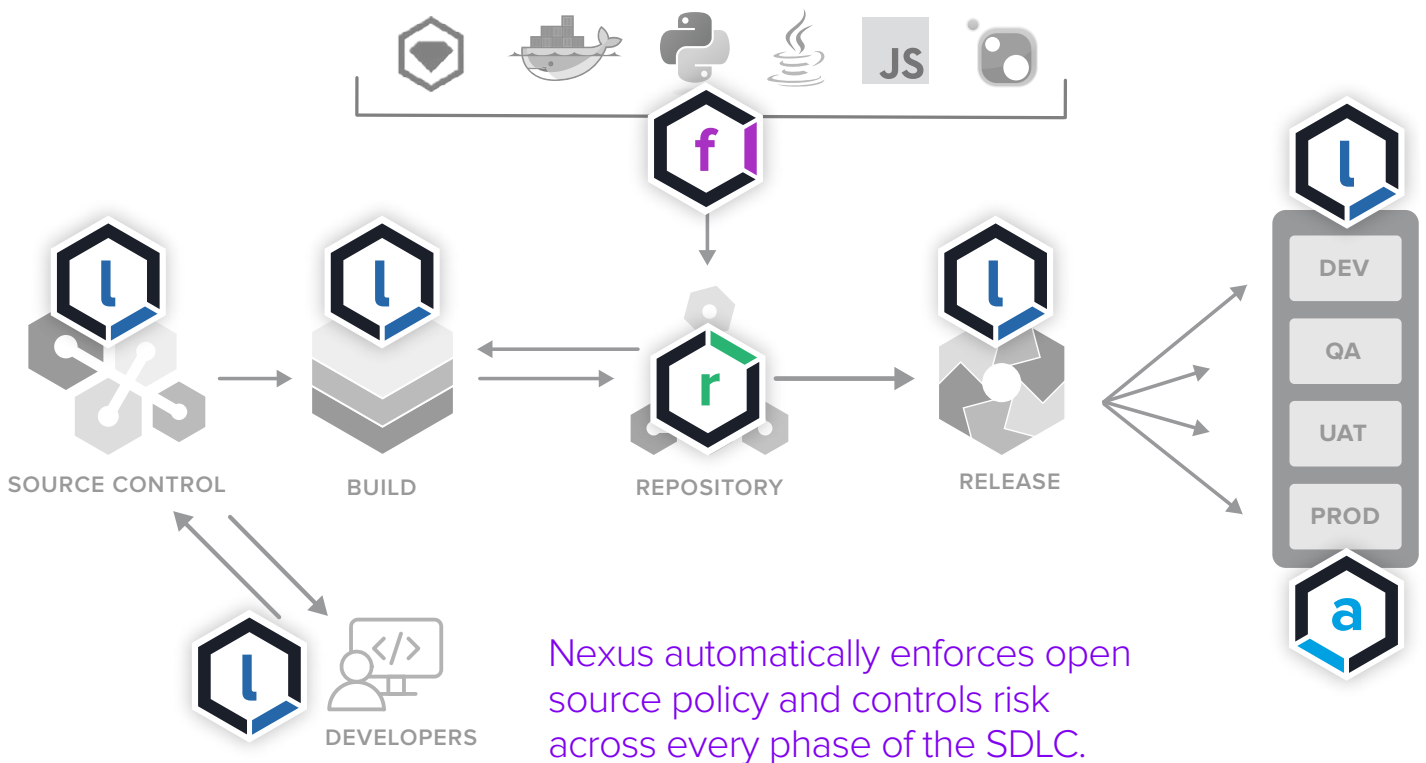


## nexus auditor

Examine OSS components within production apps.

“[Nexus] has helped developer productivity. **It's like working in the dark and all of a sudden you've got visibility.** You can see exactly what you're using and you have suggestions so that, if you can't use something, you've got alternatives. That is huge.”

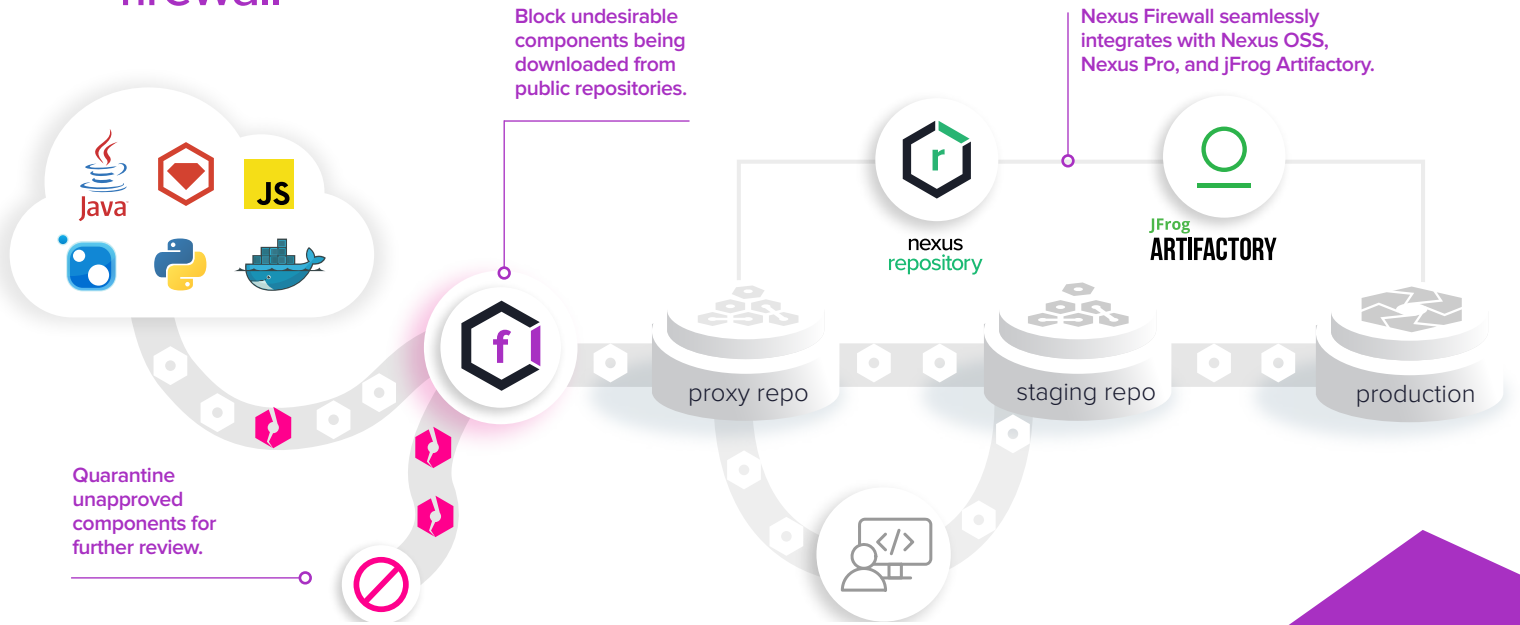
—C. CHANI (FINANCIAL SERVICES), IT CENTRAL STATION REVIEW





## THE EARLIER, THE BETTER

# Block bad components at the door.



**Repository results for maven-central**  
 Oldest evaluation 10 months ago

**738** COMPONENTS IDENTIFIED  
 100% OF ALL COMPONENTS ARE IDENTIFIED

**55** POLICY ALERTS  
 AFFECTING 86 COMPONENTS

**29** **2** **49** QUARANTINED COMPONENTS

FILTER: All Exact Unknown VIOLATIONS: Summary All Quarantined Waived

Policy Threat	Component	Quarantined
Search Name	Search Coordinates	
	commons-collections : commons-collections : 3.2.1	

Component Info Policy Licenses Vulnerabilities Labels

View Existing Waivers

Policy/Action	Constraint Name	Conditions	Waivers
Security-High	High risk CVSS score	Found security vulnerability sonatype-2015-0002 with severity 9.0. Found security vulnerability sonatype-2015-0002 with severity 9.0. Found security vulnerability sonatype-2015-0002 with status 'Open', not 'Not Applicable'. Did not find label 'custom vuln'.	Waive

Block, analyze, and selectively admit components.

Waive policy violations for component use when necessary.



**PREVENTION IS BETTER THAN A CURE.**

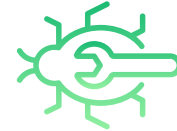
Maintain a trusted repository with Repository Health Check.



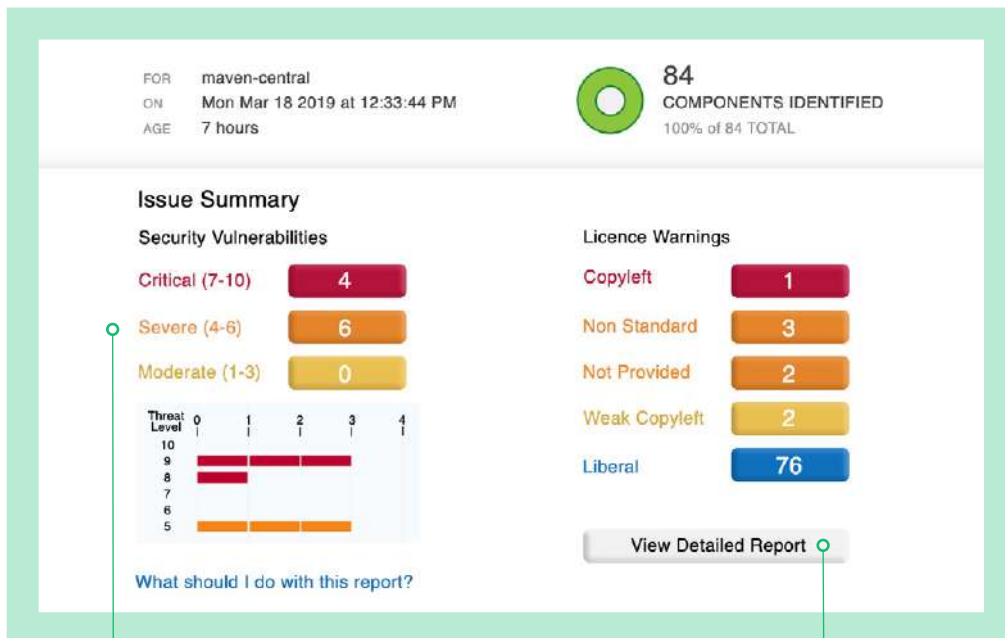
Repository Health Check (RHC) provides up-to-date component intelligence, so your teams make informed decisions early on.



Learn how often a component is being downloaded and view trending information over time.



Quickly learn the best way to remediate a vulnerable component, i.e, replace it or update it with a new version.



“It ensures our developers are utilizing safe, open-source components. Through the use of Nexus software, we know when they were downloaded and where they’re being used. **It has helped us increase the security of our applications.**”

— A. EVANS (GOVERNMENT), IT CENTRAL STATION REVIEW

Understand the overall vulnerability of your repository at quick glance.

View criticality of the vulnerable components and trending information for how often that component has been downloaded.



## EMPOWER DEVELOPERS

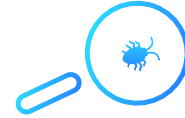
Help them make better, safer component choices early in development.



Deliver component intelligence to developers in the tools they use every day.



Choosing a safer component is as easy as using a spell checker. Just one click in your IDE or a GitHub pull request.



Early detection and remediation prevents unplanned work, security breaches and maintainability issues.

“I would give this product a nine out of ten. I’ll have a full report of artifacts—including those that are not secure—that would have been ingested into our organization. **That information is priceless.**”

—C. CHANI (FINANCIAL SERVICES), IT CENTRAL STATION REVIEW

**Easily spot risk associated with a particular component.**

Constraint	Summary
PCI 30 day	CVSS Score
Unpopular	Popularity

**Color indicates component risk severity including security, license and quality.**

Threat Level	Declared License(s)	Observed License(s)
Liberal	Apache-2.0	Apache-2.0

**Simply slide the selector to the right until a component version meets your policy guidelines.**

**Details are easy to see and understand at a glance.**

Group: org.apache.struts  
Artifact: struts2-core  
Version: 2.3.4  
Declared License: Apache-2.0  
Observed License: Apache-2.0  
Highest Policy Threat: 9 within 2 policies  
Highest Security Threat: 10 within 19 security issues  
Categorized: 2 years ago  
Match State: exact  
Identification Source: Sonatype

## NEXUS LIFECYCLE

Analyze and enforce policies *automatically*.



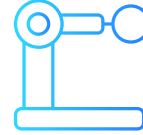
Ensure that policies are enforced as components are consumed across a variety of development tools.



Replace inefficient workflows and the burden of manual reviews.



Customize policies to meet specific compliance goals or mandates OR use our default policies to gain an immediate view of security, license, and quality risk.



Do it all with automation that supports agile and continuous goals!

**Easily create custom policies across the software lifecycle.**

**Set organization-wide policy on which violations can be dismissed and which cannot.**

**Choose the applications or types to which the policy should be applied.**

**Define precisely when the policy applies and what actions should take place.**

The screenshot shows the 'Edit Policy' interface with the following details:

- Policy Name:** License-AGPL
- Threat Level:** 10
- Policy Violation Grandfathering:**  Do not allow this policy to be grandfathered
- INHERITANCE:** This Policy Inherits to:
  - All Applications in Sandbox
  - Applications of the specified Application Categories in Sandbox
    - Distributed
    - Hosted
    - Internal
    - Trusted
- CONSTRAINTS:** AGPL (not for distributed or hosted applications) is in violation if the following is true:
  - License Threat Group is Banned
- ACTIONS:** A table defining actions for different lifecycle stages.

ACTION	PROXY	DEVELOP	BUILD	STAGE	RELEASE	OPERATE
No Action	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Warn	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**“[Nexus Lifecycle] blocks undesirable open source components from entering our development lifecycle, based on the policies that we set. It will break the build straight away. There’s no way you can ship code that introduces new vulnerabilities. We just don’t allow it at all.”**

— E. KWAN (FINANCIAL SERVICES), IT CENTRAL STATION REVIEW



## NEXUS LIFECYCLE

Verify policy compliance by knowing what components are used and where.



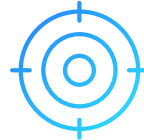
In just minutes, create an accurate software bill of materials for each application.



Identify specific components and their dependencies.



Gain access to name, license, age, popularity, known security vulnerabilities, and other metadata.



Know the exact location of any component — no more searching to see if you are impacted by a new vulnerability.

**“We’re no longer building blindly with vulnerable components.** We have awareness, we’re pushing that awareness to developers, and we feel we have a better idea of what the threat landscape looks like. Things that we weren’t even aware were vulnerabilities, we can now remediate really quickly.”

— D. DUFFY (FINANCIAL SERVICES),  
IT CENTRAL STATION REVIEW

**Welcome to the Policy-Centric Application Report Preview**

This is the preview of the new Policy-Centric Application Report. Documentation can be found [here](#). We'd love to hear what you think of this new report, if you have any comments you can [submit them here](#).

### Appfuse Build Report

2019-03-11

5 12 3 **20 VIOLATIONS** Affecting 10 components

53 **COMPONENTS** 96% of all components identified

0 **GRANDFATHERED** violations

THREAT	POLICY	COMPONENT
9	Security-High	commons-fileupload : commons-fileupload : 1.2.1
9	Security-High	org.springframework : spring-web : 3.0.5.RELEASE
9	Security-High	taglibs : standard : 1.1.2
7	Security-Medium	org.springframework : spring-context : 3.0.5.RELEASE
7	Security-Medium	org.springframework : spring-core : 3.0.5.RELEASE
7	Security-Medium	org.springframework : spring-webmvc : 3.0.5.RELEASE
7	Security-Medium	org.springframework.security : spring-security-core : 3.1.2.RELEASE
0	None	commons-collections : commons-collections : 3.1
0	None	javax.serviet : jstl : 1.2

**Aggregation**

- Aggregated by Component
- All Violations

**Filters**

- Proprietary (2)
- Component Match State (3)
- Violation State (4)
- Policy Types (1 of 4)
  - all/none
  - Security
  - License
  - Quality
  - Other
- Policy Threat Level (0-10)

**View the violations against various policy types.**

**Color codes identify critical (red), severe (orange) and moderate (yellow) risk levels. Severity criteria is configurable based on policy settings.**

**Identify the component group, and the specific component and version used in any application.**

**Developers view the threat that a violation has against an organization-wide policy.**

## NEXUS LIFECYCLE

Get visibility and transparency for quick remediation.



One dashboard easily filtered to support development, operations, security, and compliance.



Prioritize remediation and development work based on detailed intelligence.



Track progress and trends for defects opened, fixed, waived, and discovered.



Reduce your technical debt and ease the maintenance burden.

**“My advice is ‘do it yesterday.’ You save yourself a lot of money.** Even during one, two, or three weeks, it’s going to cost you a lot of money to fix the security vulnerabilities that you are ingesting in your development lifecycle. You could be avoiding that by using a product like Lifecycle.”

— C. CHANI (FINANCIAL SERVICES),  
IT CENTRAL STATION REVIEW

Easy to understand description written for developers by developers.

In-depth research includes detailed detection and remediation guidance.

The screenshot displays the Nexus Lifecycle dashboard with a 'Vulnerability Information' modal window open. The dashboard header shows 738 components identified, 56 policy alerts, 29 vulnerabilities, 2 high-severity items, and 50 quarantined components. The modal window provides detailed information for a vulnerability in the 'License-Banned' category, marked as 'Security-High'. The vulnerability is related to 'jackson-databind' and involves Remote Code Execution (RCE). The modal includes sections for 'Explanation', 'Detection', and 'Recommendation', along with a 'Close' button.

**Vulnerability Information**

...sending the maliciously created input to the readValue method of the ObjectMapper. This issue extends the previous flaw CVE-2017-7525 by blacklisting more classes that could be used maliciously.

**Explanation**

jackson-databind is vulnerable to Remote Code Execution (RCE). The createBeanDeserializer() function in the BeanDeserializerFactory class allows untrusted Java objects to be deserialized. A remote attacker can exploit this by uploading a malicious serialized object that will result in RCE if the application attempts to deserialize it.

Note: This vulnerability exists due to the incomplete fix for CVE-2017-7525

**Detection**

The application is vulnerable by using this component, when default typing is enabled and passing in untrusted data to be deserialization.

Note: Spring Security has provided their own fix for this vulnerability (CVE-2017-4995). If this component is being used as part of Spring Security, then you are not vulnerable if you are running Spring Security 4.2.3.RELEASE or greater for 4.x or Spring Security 5.0.0.M2 or greater for 5.x.

**Recommendation**

There is no non vulnerable version of this component. Despite there being a fix provided by Jackson, it uses a black-list approach. If there is another class not black-listed which performs deserialization on the classpath, then this may lead to code

Close

“There is a feature called Continuous Monitoring. Because of this feature, as time goes on we’ll be able to know whether a platform is still secure or not. **It’s integrated, it’s proactive, it’s exactly what you want for a security product.**”

— C. CHANI (FINANCIAL SERVICES), IT CENTRAL STATION REVIEW

## NEXUS LIFECYCLE

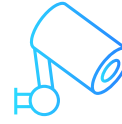
# Continuously monitor for new defects.



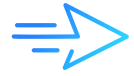
An automated early warning system to identify newly discovered defects.



Detailed intelligence on vulnerabilities including precise root cause and component dependencies.



Ongoing monitoring and alerts of new vulnerabilities based on component, risk level, or applications affected.



Improve incident response times with precise identification of components and apps to be remediated.

View a list of all components that have policy violations in a particular stage. Identify which apps include those components.

Identify the total risk of each component as well as a breakdown by severity to determine which components should be remediated first.

Easily search for components based on application stage and policy types.

NAME	AFFECTED APPS	TOTAL RISK	CRITICAL	SEVERE	MODERATE	LOW
commons-httpclient : commons-httpclient : 3.1	11	200	81	115	6	0
org.apache.struts : struts2-assembly : 2.0 : all : 2.3.14	4	150	96	48	6	0
org.apache.struts : struts2-blank : war : 2.3.14	4	130	76	48	6	0
org.apache.struts : struts2-showcase : war : 2.3.14	4	130	76	48	6	0
org.apache.struts : struts2-partlet : war : 2.3.14	4	130	76	48	6	0
org.apache.struts : struts2-rest-showcase : war : 2.3.14	4	130	76	48	6	0
axis : axis : 1.2	6	126	54	72	0	0
org.apache.struts : struts2-mailreader : war : 2.3.14	4	125	76	43	6	0
commons-collections : commons-collections : 3.1	10	122	98	24	0	0
org.apache.struts : struts2-core : 2.3.14	4	122	76	43	3	0
commons-collections : commons-collections : 3.2.1	9	99	61	18	0	0
org.apache.struts : struts2-core : 2.3.14	4	99	66	33	0	0
org.springframework : spring-context : 2.5.6.SEC03	6	94	36	58	0	0
org.apache.httpcomponents : httpclient : 4.2.5	6	94	36	58	0	0
org.springframework : spring-web : 2.5.6.SEC03	6	94	36	52	6	0
org.apache.jackrabbit : jackrabbit-webdav : 2.5.2	6	87	36	51	0	0

# Integrations? You better believe It.

We work where you work.



# 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](http://www.sonatype.com)**

## Headquarters

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

## Virginia Office

8281 Greensboro Dr Suite 630  
McLean, VA 22102

## 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](http://www.sonatype.com)  
Sonatype Copyright 2019  
All Rights Reserved.



## nexus vulnerability scanner

## Better or the best? You decide.

Test drive the power of Nexus Intelligence in five minutes.

Run a free Nexus Vulnerability Scan to learn about vulnerabilities in an app (yours or one of ours).

**Try it free at [www.sonatype.com/appscan](http://www.sonatype.com/appscan).**

Bank X Better Payments - 2017-02-23 - Stage Release Report

Policy Threat	Component	Filename	Popul...	Age	Release History
Security-High	aws: aws: 1.2	aws-1.2.jar	11.5 y		
	commons-collections: commons-collections: 3.1	commons-collections-3.1.jar	11.0 y		
	commons-fileupload: commons-fileupload: 1.2.1	commons-fileupload-1.2.1.jar	9.3 y		
Component-Unknown	WebGee: 5.4.4.3-SNAPSHOT	WebGee-5.4.4.3-SNAPSHOT.jar	No Popularity Data		
None	aws: aws: 1.2	aws-1.2.jar	11.5 y		
	aws: aws: 1.2	aws-1.2.jar	11.0 y		
	aws: aws: 1.2	aws-1.2.jar	11.5 y		
	commons-beanutils: commons-beanutils: 1.8	commons-beanutils-1.8.jar	11.5 y		
	commons-digester: commons-digester: 1.4.1	commons-digester-1.4.1.jar	11.8 y		
	commons-discovery: commons-discovery: 0.2	commons-discovery-0.2.jar	11.0 y		
	commons-io: commons-io: 1.4	commons-io-1.4.jar	9.3 y		
	commons-logging: commons-logging: 1.0.4	commons-logging-1.0.4.jar	11.0 y		
	ecs: ecs: 1.4.2	ecs-1.4.2.jar	11.5 y		
	example: example: 1.1	Example-1.1.jar	1.0 y		No Popularity Data
	example: example: 1.1	Example-1.1.jar	1.5 y		No Popularity Data
	hadoop: hadoop: 1.8.0.10	hadoop-1.8.0.10.jar	9.0 y		