

Welcome to Sonatype Help

Table of Contents

Table of Contents	1
Repository Manager.....	2
IQ Server	2
Important Announcements	2
Struts2 Frequently Asked Questions	3
Nexus Lifecycle Customers	3
Nexus Firewall Customers	4
Nexus Repository Manager Pro Customers.....	5
Solutions vs. Products.....	6
Understanding Sonatype Vulnerability Data.....	8
What is Sonatype Vulnerability Data?	8
How does Sonatype provide high quality data?	8
What Data Does Sonatype Provide?	8
How is a vulnerability score / severity calculated?.....	9
Where are the Source Components?	9
When is Vulnerability Data Available?	9
How do I Access Vulnerability Information?	10
How do I Use Vulnerability Information?	11
Copyright	12



Repository Manager

[Release Notes](#)¹

[Documentation \(NXRM 3\)](#)²

[Documentation \(NXRM 2\)](#)³

[Integrations](#)⁴

[Quick Start Guide](#)⁵



IQ Server

[Release Notes](#)⁶

[Documentation](#)⁷

[Integrations](#)⁸

[Firewall Quick Start](#)⁹

[Lifecycle Quick Start](#)¹⁰

Important Announcements

Check here for Sonatype announcements on all of our products:

- [Struts2 Frequently Asked Questions](#) (see page 3)

¹ <https://help.sonatype.com/display/NXRM3/Release+Notes>

² <https://help.sonatype.com/display/NXRM3>

³ <https://help.sonatype.com/display/NXRM2>

⁴ <https://help.sonatype.com/display/NXI>

⁵ <https://help.sonatype.com/display/SL/Proxying+Maven+and+NPM+Quick+Start+Guide>

⁶ <https://help.sonatype.com/display/NXIQ/Release+Notes>

⁷ <https://help.sonatype.com/display/NXIQ>

⁸ <https://help.sonatype.com/display/NXI>

⁹ <https://help.sonatype.com/display/NXIQ/Nexus+Firewall+Quick+Start>

¹⁰ <https://help.sonatype.com/display/NXIQ/Nexus+Lifecycle+Quick+Start>

Struts2 Frequently Asked Questions

Nexus Lifecycle Customers

How do I determine if my organization is impacted by any Struts2 vulnerabilities?

If you've performed an analysis on all configured applications since the latest disclosure, or have [continuous monitoring](#)¹¹ enabled for Security-High policies, then your application has been analyzed against the CVEs. If you are using Struts and did not have a violation raised, you can rest assured you are not affected (assuming you're using our [reference policies](#)¹²).


What if I have not yet performed an analysis and I do not want to wait for the next build?

You can trigger monitoring to manually run immediately by issuing the following request to the IQ Servers administrative port (default is 8071):

```
$ curl -X POST http://localhost:8071/tasks/triggerPolicyMonitor
```

The following response will indicate it is complete:

Completed manual Policy Monitor execution

 You will need access to the [administrative port](#)¹³ used for IT debugging and operations, not the usual IQ Server administrator role.

How can I find a list of my applications that contain Struts?

- **Option 1:** Use the Dashboard components view as described in the [IQ Dashboard](#)¹⁴ topic.
- **Option 2:** Use the public REST API to search for the component. See [Component Search REST APIs - v2](#)¹⁵ for how to create a call to search for a specific Component GAV. For example:
org.apache.struts:struts2-rest-plugin:*:*:

11 <https://help.sonatype.com/display/NXIQ/Continuous+Monitoring+of+Apps>

12 <https://help.sonatype.com/display/NXIQM/Policy+Management#PolicyManagement-ReferencePolicySet>

13 https://help.sonatype.com/display/NXIQ/IQ+Server+Configuration#IQServerConfiguration-HTTP_Config

14 <https://help.sonatype.com/display/NXIQ/Dashboard>

15 <https://help.sonatype.com/display/NXIQ/Component+Search+REST+APIs+-+v2>

How should we remediate this issue?

Upgrade the component to the newly released non-vulnerable version. Please reference the in-product security vulnerability information for additional details for mitigating the vulnerability exposure.

How can we prevent future exploits?

It is almost impossible to avoid zero-day vulnerabilities. There will always be a time gap between the zero-day discovery and public reporting. There is another time gap between the public release and the vulnerability appearing in evaluation results. Immediate notification is a key element for limiting potential impact. Sonatype is often aware in advance of a new vulnerability announcement, enabling us to provide notice within IQ Server prior to the issue being released publicly. In other instances, we must perform the issue identification and research after the issues are publicly released. In these cases, we strive to include the vulnerability in our data within a few hours of announcement.

There are additional preventative measures that can be established within your development practices that will better prepare your organization for these situations and decrease your time to response. Contact Customer Success to learn more about how Nexus Lifecycle and associated best practices can help.

Nexus Firewall Customers

How do I determine if my organization is impacted by the latest vulnerability disclosure?

Firewall can audit component downloads from a given proxy repository (Java, .NET, npm, Python). Users can view a report that contains all components, which have been previously downloaded to your Nexus Repository through that applicable proxy repository.

This report can be reviewed for any instances of Struts. Users can search for a particular Struts component (E.g. org.apache.struts:struts2-rest-plugin:*). In addition, the Firewall results include Sonatype-curated vulnerability information - for this CVE and others - only available to Sonatype "Firewall" and "Lifecycle" customers.

If this component is found, it indicates it was previously downloaded into your Nexus Repository. As a result, the component is available to applications with privileges to access that proxy repository. To associate a component to a specific application, please visit Sonatype's "[Application Health Check \(AHC\)](#)¹⁶" a no-cost service. To automate this monitoring across all applications, see "Nexus Lifecycle" above.

¹⁶ <https://www.sonatype.com/software-bill-of-materials>

How should we remediate this issue?

Upgrade the component to the newly released non-vulnerable version. Please reference the in-product security vulnerability information for additional details for mitigating the vulnerability exposure.

How can Firewall help with other known vulnerabilities?

In addition to auditing component downloads, Nexus Firewall is designed to quarantine component download requests based on IQ Server policy configuration. You can configure policy to quarantine new component downloads for known vulnerable versions of any component based on any range of criticality. Check out "[How to Keep Vulnerable Versions of Struts Out of Your Nexus Repository](#)¹⁷" for guidance on how this can be achieved.

Nexus Repository Manager Pro Customers

How do I determine if my organization is impacted by the latest vulnerability disclosure?

[Repository Health Check](#)¹⁸ (RHC) can audit component downloads from a given proxy repository (Java, .NET, npm, Python). Users can view a report that contains all components, which have been previously downloaded to your Nexus Repository through that applicable proxy repository.

This report can be reviewed for any instances of Struts. Users can search for a particular Struts component (E.g. org.apache.struts:struts2-rest-plugin:*). In addition, the RHC report includes links to the associated CVE.

If this component is found, it indicates it was previously downloaded into your Nexus Repository. As a result, the component is available to applications with privileges to access that proxy repository. To associate a component to a specific application, please visit Sonatype's "[Application Health Check](#)¹⁹ (AHC)" a no-cost service. To automate this monitoring across all applications, see "Nexus Lifecycle" above.

How should we remediate this issue?

Upgrade the component to the newly released non-vulnerable version. Please reference the CVE security vulnerability information for additional details for mitigating the vulnerability exposure.

¹⁷ <https://blog.sonatype.com/how-to-keep-vulnerable-versions-of-struts-out-of-your-nexus-repository>

¹⁸ <http://blog.sonatype.com/how-to-use-the-new-repository-health-check-2.0>

¹⁹ <https://www.sonatype.com/software-bill-of-materials>

How can Repository Health Check (RHC) help with other known vulnerabilities?

[Enabling RHC²⁰](#) on all supported repository types provides insight into component downloads across your proxy repositories. In addition, the report includes trend analysis determined by month to month asset downloads.

Additional information related to recent Struts2 vulnerability announcements

Sonatype Statements:

- <http://blog.sonatype.com/sonatype-statement-struts2-and-equifax-breach>
- <https://blog.sonatype.com/deja-vu-all-over-again-another-new-apache-struts-vulnerability-cve-2018-11776>

CVE-2018-11776 Disclosure

- <https://semml.com/news/apache-struts-CVE-2018-11776>

Facebook Live interview (8/22/18) with Sonatype CTO, Brian Fox, discussing CVE-2018-11776

- <https://www.facebook.com/Sonatype/videos/846420692229318/UzpfSTM5NDc0OTUyMDU2MzU0OToxODk1NTU4OTQ3MTQ5MjU4/>

OWASP Podcast (9/8/17) with Sonatype CTO, Brian Fox and Matt Konda, Chair, OWASP Board of Directors, regarding CVE-2017-12611:

- <http://blog.sonatype.com/what-you-should-know-about-the-struts-2-vulnerability-announcement-video>

Additional Sonatype blog posts on the 2017 Equifax breach and Struts2 vulnerabilities

- <http://blog.sonatype.com/alert-three-things-to-know-about-the-newest-struts2-vulnerability>
- <http://blog.sonatype.com/struts2-vulnerability-cracks-equifax>
- <http://blog.sonatype.com/bracing-for-impact-in-more-ways-than-one-apache-struts2-s2-053>

Apache statement on Equifax:

- <https://blogs.apache.org/foundation/entry/apache-struts-statement-on-equifax>

Solutions vs. Products

You may have noticed that there is a difference between the names used on our website (solutions), and the names you will find on our help site (products).

In general, when we are talking about a solution, we are referring a particular license (Nexus Lifecycle vs. Nexus Firewall or Nexus Repository OSS vs. Nexus Repository Pro) and the features it unlocks. In contrast,

²⁰ <http://blog.sonatype.com/how-to-use-the-new-repository-health-check-2.0>

when we describe a product, we specifically mean the thing you will install Nexus Repository (Manager) and Nexus IQ (Server).

i While not a license in the same sense, the principal for Nexus Repository is the same, meaning we treat Pro as a license, which would enable features within the Nexus Repository (Manager) product. However, there is a slight difference between 2 and 3. For Nexus Repository 2, there are separate product installs that support each license. In contrast, for Nexus Repository 3, there is a single install that will provide OSS features by default, and allow a Pro license to be added, unlocking additional functionality.

Of course, this can still be a bit confusing, so we've broken down the various solutions (licenses) available, and their corresponding product in the table below.

Solution (License)	Product (What's Installed)
Nexus Repository OSS 2	Nexus Repository (Manager) OSS 2
Nexus Repository Pro 2	Nexus Repository (Manager) Pro 2
Nexus Repository OSS 3	Nexus Repository (Manager) 3
Nexus Repository Pro 3	Nexus Repository (Manager) 3
Nexus Auditor	Nexus IQ (Server)
Nexus Firewall	Nexus IQ (Server)
Nexus Lifecycle	Nexus IQ (Server)

As you may have noticed, in some cases the same product is installed regardless of the license. To help understand which features are unlocked by a particular license, we've included matrices to assist:

[Repository Manager Feature Matrix](https://help.sonatype.com/display/NXRM3/Repository+Manager+Feature+Matrix)²¹

[IQ Download and Compatibility](https://help.sonatype.com/display/NXIQ/Download+and+Compatibility)²²

²¹ <https://help.sonatype.com/display/NXRM3/Repository+Manager+Feature+Matrix>

²² <https://help.sonatype.com/display/NXIQ/Download+and+Compatibility>

Understanding Sonatype Vulnerability Data

What is Sonatype Vulnerability Data?

Sonatype creates its data using a proprietary, automated vulnerability detection system that monitors, aggregates, correlates, and incorporates machine learning from publicly available information. We gather data from various sources including the National Vulnerability Database, website security advisories, email lists, GitHub events from all open source projects, blogs, OWASP, OSS Index, Twitter, and customer reports. We have evaluated many paid-for services and have found the quality and precision of the data to be of limited value, driving our decision to build an intelligent, automated vulnerability detection system. The Sonatype Data Research team is not in the business of simply aggregating public security related feeds – we create the precise data we use.

How does Sonatype provide high quality data?

There are two considerations for data quality: (1) content of the security advisory and (2) precision of associating the content to the correct artifact. Automated decisions require extremely precise artifact identification and corresponding association of security information. Without accurate identification and association there is a high degree of false positives. We recently conducted a study of 6000 of the most popular Java components and found that name-based security association algorithms used by every tool other than Sonatype resulted in:

- 4500 correct non-issue identifications
- 1034 true positives
- 5330 false positives when the advisory identified CPE was part of the component name
- 2969 false negatives when the advisory identified CPE was not in the component name

False positives incur unnecessary research and upgrade costs. False negatives leave you at risk because there are no indicators that show you may be at risk. Sonatype uses a combination of automated identification and human research that eliminates false positives and negatives. This results in savings in research time to prove false positives and rework time to upgrade when not required.

What Data Does Sonatype Provide?

- The source of the advisory: Sonatype Security Research or the National Vulnerability Database
- The severity of the issue: CVSS and scoring system version and the source of the score creation
- The Common Weakness Enumeration (CWE)
- The exact description from the advisory

- A detailed explanation of the advisory risk and the attack vector (because the advisory description is often very poor)
- How to determine if you are vulnerable
- A recommendation on how to fix or work-around the issue
- The root cause of the issue; the exact class and vulnerable version range that was found in your code
- Publicly known attack vectors or exploits; additional resources that describe the exact issue

How is a vulnerability score / severity calculated?

Sonatype uses the [Common Vulnerability Scoring System](#)²³ (CVSS) to score vulnerabilities.

If a vulnerability identifier is prefixed with *SONATYPE*, then the vulnerability severity is its CVSS version 3 score.

If a vulnerability identifier is prefixed with *CVE*, then the vulnerability severity is its CVSS version 2 score.

Sonatype plans to ultimately migrate all CVSS version 2 scores to version 3. If a version 3 score is not available, the score will remain version 2.

Where are the Source Components?

Component binaries come from popular repositories like [Central](#)²⁴, [NuGet.org](#)²⁵, [npmjs.org](#)²⁶, Fedora EPEL, and [PyPI](#)²⁷. We will also ingest components directly from GitHub, and other project download sites, when nominated by customers.

Binary repositories provide the ability to extract information like declared licenses, popularity, and release history. Additional component metadata comes from a variety of sources including direct research.

When is Vulnerability Data Available?

Sonatype Data Services are continuously updated, allowing the most recent data to be visible the instant a Nexus Lifecycle analysis occurs. This is true for both newly published components and newly discovered security issues. We have two processing queues for security vulnerabilities to ensure immediate availability of security data to our customers:

Fast Track - Our automated vulnerability detection systems process the various data sources each day. Upon issue discovery, the issue is validated by a researcher to ensure the correct component was identified, a brief

²³ https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System

²⁴ <http://search.maven.org/>

²⁵ <http://nuget.org/>

²⁶ <http://npmjs.org/>

²⁷ <https://pypi.python.org/pypi>

issue description exists, and the vulnerable version range matches the advisory. This process generally makes newly discovered vulnerabilities available in 1-3 days depending on severity of the issue.

Deep Dive - The deep dive queue is a more methodical approach to ensure the issue has a clear explanation and fix recommendation. This is also where the source code of each issue is investigated to ensure the vulnerable version range is accurate. This process generally takes 5+ days, but can take less for issues deemed critical.

How do I Access Vulnerability Information?

Sonatype-enriched vulnerability data is available from the IQ Server [Application Composition Report](#)²⁸. Select the *Security Issues* tab and then select the problem code you're investigating:

Test123 - 2017-09-22 - Build Report

Summary	Policy Violations	Security Issues	License Analysis
---------	-------------------	-----------------	------------------

Threat Level ▾	Problem Code	Component	Filename	Status
Search Level	Search Code	Search Component	Search Filename	Search Status
9	CVE-2007-4575	hsqldb : hsqldb : 1.8.0.7	hsqldb-1.8.0.7.jar	Open
	SONATYPE-2015-...	commons-collections : commons-collections : 3.1	commons-collections-3.1.jar	Open
8	CVE-2017-7525	com.fasterxml.jackson.core : jackson-databind : 2.0.4	jackson-databind-2.0.4.jar	Open
7	CVE-2015-5211	org.springframework : spring-webmvc : 3.2.4.RELEASE	spring-webmvc-3.2.4.RELEASE.jar	Open
	CVE-2014-0114	commons-beanutils : commons-beanutils : 1.6	commons-beanutils-1.6.jar	Open
	CVE-2014-0050	commons-fileupload : commons-fileupload : 1.2.2	commons-fileupload-1.2.2.jar	Open
	CVE-2015-0254	javax.servlet : jstl : 1.2	jstl-1.2.jar	Open
	CVE-2016-1000031	commons-fileupload : commons-fileupload : 1.2.2	commons-fileupload-1.2.2.jar	Open
	CVE-2013-2186	commons-fileupload : commons-fileupload : 1.2.2	commons-fileupload-1.2.2.jar	Open
	SONATYPE-2014-...	angular 1.2.17	angular.js	Open
	CVE-2016-3092	commons-fileupload : commons-fileupload : 1.2.2	commons-fileupload-1.2.2.jar	Open
	SONATYPE-2014-...	angular 1.2.16	angular.min.js	Open
	CVE-2015-0254	taglibs : standard : 1.1.2	standard-1.1.2.jar	Open
6	CVE-2014-0054	org.springframework : spring-web : 3.2.4.RELEASE	spring-web-3.2.4.RELEASE.jar	Open
	SONATYPE-2014-...	angular 1.2.16	angular.min.js	Open
	SONATYPE-2016-...	angular 1.2.16	angular.min.js	Open
	SONATYPE-2016-...	angular 1.2.17	angular.js	Open
	SONATYPE-2014-...	angular 1.2.17	angular.js	Open

Showing all 40 rows

Then view the detailed Vulnerability Information:

²⁸ <https://help.sonatype.com/display/NXIQ/Application+Composition+Report>

Vulnerability Information

Source
Sonatype Data Research

Severity
Sonatype CVSS 3.0: 9.0

Weakness
Sonatype CWE: [502](#)

Explanation
Due to the behavior of `InvokerTransformer`, an arbitrary code execution attack may be executed against any application performing deserialization of user supplied objects when `commons-collections` is on the classpath.

The intended behavior of `InvokerTransformer` is to allow for the invocation of any method on the Java classpath. The `InvokerTransformer` class implements `Serializable` and therefore can be included in a serialized object. A combination of the `InvokerTransformer`'s intended functionality and because it is serializable allows an attacker to embed malicious content, such as `Runtime.getRuntime().exec()` via Java reflection, allowing arbitrary code execution.

Note: CVE-2015-7501 has been issued for this vulnerability.

Detection
The application is vulnerable if it allows deserialization of untrusted data.

Recommendation
We recommend upgrading to a version of this component that is not vulnerable to this specific issue.

A potential workaround is to remove `commons-collections` from the classpath or to remove the `InvokerTransformer` class from the `common-collections` jar file.

Note: This is not specifically a `commons-collections` issue. Any serializable object that allows reflection (dynamic method invocation) or execution of dangerous functionality will be subject to the same exploit.

Categories
Functional
Data

Root Cause
`commons-collections-3.1.jar` <=> `InvokerTransformer.class` : [3.1,3.2.1]

Advisories
Project: http://mail-archives.us.apache.org/mod_mbox/www-announce/201...
Project: <https://issues.apache.org/jira/browse/COLLECTIONS-580>
Third Party: <https://blog.codecentric.de/en/2015/11/comment-on-the-so-cal...>
Attack: <http://foxglovesecurity.com/2015/11/06/what-do-weblogic-webs...>

Close

You can also access this information from the *Vulnerabilities* tab of the [Component Information Panel](#)²⁹.

How do I Use Vulnerability Information?

The important thing to remember is that evaluating your application and seeing security vulnerabilities should create motivation for further investigation.

For example, if it's recommended to do a component upgrade, use the CIP to identify a recommended non-vulnerable, popular version.

Component Info

Policy

Similar


Occurrences

Licenses

Vulnerabilities

Labels

Audit Log



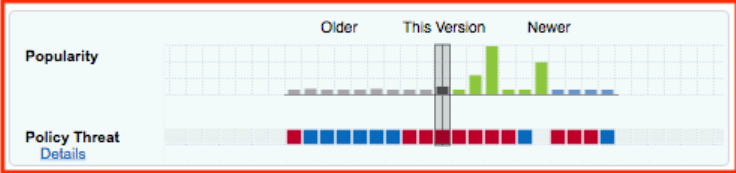
Group: **commons-collections**
Artifact: **commons-collections**
Version: **3.1**
Declared License: **Not Declared**
Observed License: **Apache-2.0**
Effective License: **Apache-2.0**
Highest Policy Threat: **9** within 2 policies
Highest CVSS Score: **9**
Cataloged: **12 years ago**
Match State: **exact**
Identification Source: **Sonatype**

Popularity

Policy Threat

Details

Older This Version Newer



²⁹ <https://help.sonatype.com/display/NXIQ/The+Component+Information+Panel>

If the new version has the same API as the previous component, simply run unit and integration tests and make sure everything passes to successfully remediate the policy violation.

Copyright

Copyright © 2008-present, Sonatype Inc. All rights reserved. Includes the [third-party code listed here](#).

Sonatype and Sonatype Nexus are trademarks of Sonatype, Inc.

Sonatype Nexus Repository Manager OSS™, Nexus Repository Manager Pro™, Nexus Lifecycle™, Nexus Auditor™, Nexus Firewall™, IQ Server™, and all Nexus-related logos as well as Sonatype CLM are trademarks or registered trademarks of Sonatype, Inc., in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle, Inc., in the United States and other countries.

IBM® and WebSphere® are trademarks or registered trademarks of International Business Machines, Inc., in the United States and other countries.

Eclipse™ is a trademark of the Eclipse Foundation, Inc., in the United States and other countries.

[Apache Maven](#) and [Maven](#) are trademarks of the Apache Software Foundation. [M2Eclipse](#) is a trademark of the Eclipse Foundation. All other trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear, and Sonatype, Inc. was aware of a trademark claim, the designations have been printed in caps or initial caps.

While every precaution has been taken in the preparation of this content, the publisher and authors assume no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.