Welcome to Sonatype Help

Table of Contents

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 2)

Struts2 Frequently Asked Questions

[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://guides.sonatype.com/repo3/quick-start-guides/
[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

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/Configuring#Configuring-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 RHC[20] 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://semmle.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).

> ⓘ 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[21]

IQ Download and Compatibility[22]

Copyright

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

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

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.