

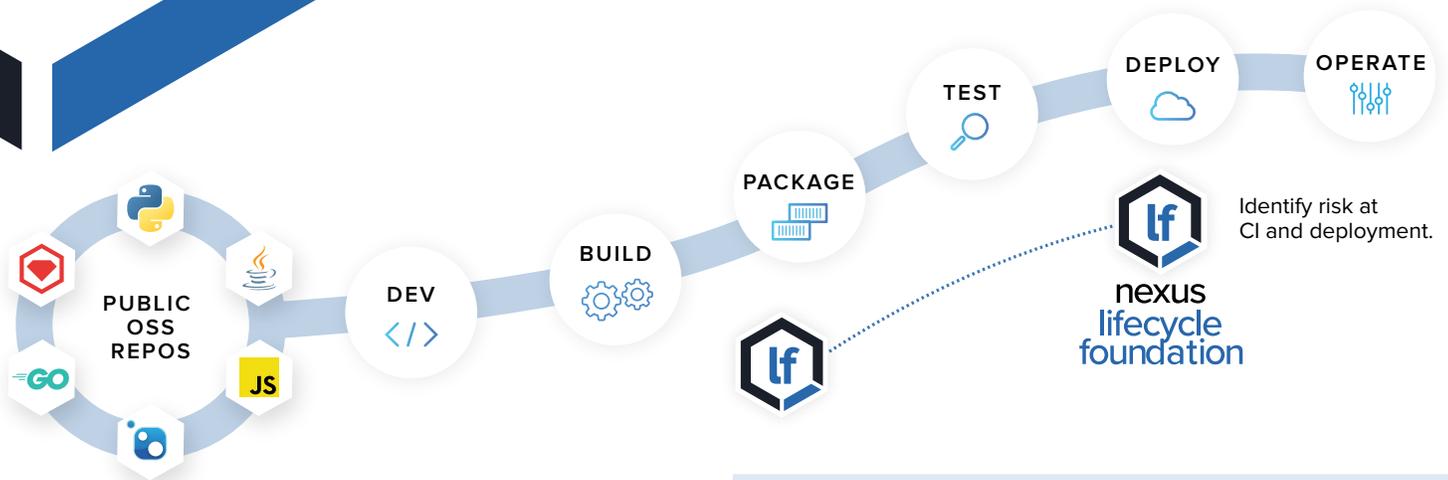


Nexus Lifecycle Foundation

Identify open source risk in your applications.

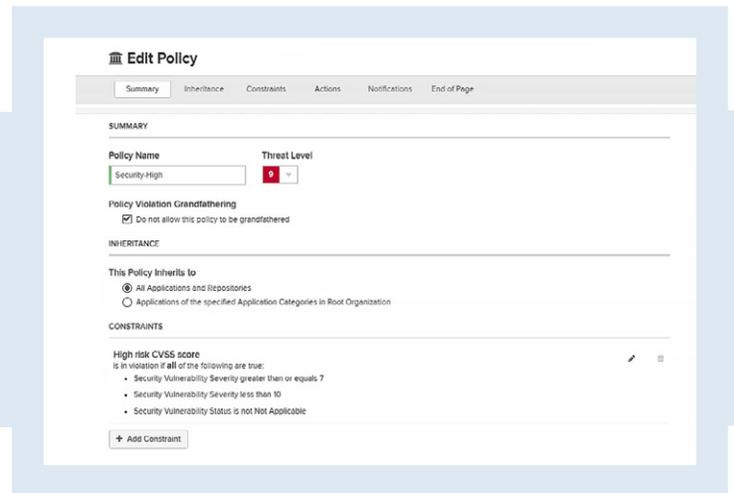
It's no secret. Developers use open source — in fact, 85% of a modern application is comprised of open source components, and unfortunately *one in ten* open source component downloads contain a known security vulnerability. Given this inherent risk, how do organizations ensure they are secure?

Nexus Lifecycle Foundation provides visibility into open source risk before it's too late. Integrated into your CI/CD pipeline, you can clearly see if developers are using components that violate your open source policies.



Create Customized Policies

Create custom security, license, and architectural policies based on application type or organization to automatically identify risk within your applications.



“We have seen a return on our investment.

In some cases, where we’ve needed to find out the footprint of a certain library across our enterprise, we’ve been able to do that research in seconds or minutes, rather than long, drawn-out processes with people and teams involved to hunt it down through source code and the like.”

— R. WEBSTER (Financial Services), IT Central Station Review



Integrate Into Existing CI/CD Pipeline

Integrates with your favorite tools to identify risk during build times, before it's too late.



www.sonatype.com

Automatically Generate a Software Bill of Materials

Verify policy compliance by knowing what components are used and where. In just minutes, generate a precise software BoM for each app to identify every open source component along with its dependencies.

| THREAT | POLICY | COMPONENT |
|--------|----------------------|---|
| 9 | License-None | axis : axis-ext : 1.2 |
| 9 | License-None | javax.xml : j2m : 1.3.1 |
| 9 | Security-High | axis : axis : 1.2 |
| 9 | Security-High | commons-beanutils : commons-beanutils : 1.6 |
| 9 | Security-High | commons-collections : commons-collections : 3.2.1 |
| 8 | License-CopyLeft | javax.mail : mailapi : 1.4.2 |
| 7 | Security-Medium | commons-fileupload : commons-fileupload : 1.3.3 |
| 7 | Security-Medium | javax.mail : mail : 1.4.2 |
| 5 | License-Non Standard | commons-logging : commons-logging : 1.0.4 |
| 5 | License-Non Standard | hsqldb : hsqldb : 1.9.0.10 |
| 1 | Architecture-Quality | apache-log4j : log4j : 1.2.8 |
| 1 | Architecture-Quality | axis : axis-jaxrpc : 1.2 |
| 1 | Architecture-Quality | axis : axis-saaj : 1.2 |
| 1 | Architecture-Quality | commons-digester : commons-digester : 1.4.1 |

Repository results for maven-central
 Oldest evaluation 7 months ago

738 COMPONENTS IDENTIFIED
 100% OF ALL COMPONENTS ARE GUARANTEED

56 POLICY ALERTS | 29 POLICY VIOLATIONS | 2 POLICY CRITICAL | 50 GUARANTEED COMPONENTS

Vulnerability Information

Warning: The maliciously crafted 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 deserialized.

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.

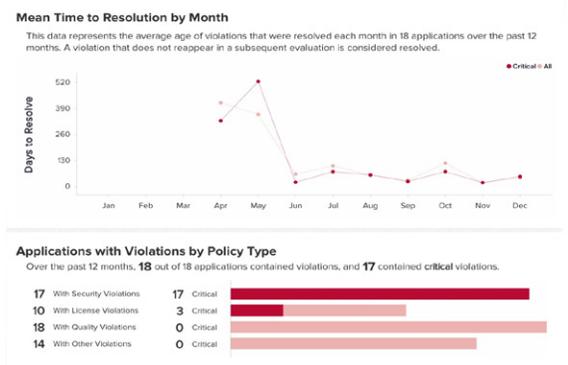
Recommendation
 There is no non vulnerable version of this component. Despite there being a fix provided by Jackson, it uses a black-list approach. If there is another class not black-listed which performs deserialization on the classpath, then this may lead to code execution.

Eliminate Risk with Expert Remediation Guidance

Sonatype employs more than 65 security researchers to review every open source vulnerability and provide expert remediation guidance. Whenever new vulnerabilities are disclosed or discovered, our team immediately validates the exploit path, identifies the root cause, and creates actionable information to help organizations (and development teams) evaluate, triage, and remediate threats faster than adversaries can attack.

View Trends Related to Mean Time to Resolution (MTTR)

Demonstrate risk reduction to senior management with a report that shows violation trends over time and how quickly they are being remediated.



Key Benefits of Nexus Lifecycle Foundation

- ✓ Security teams sleep better at night knowing exactly what open source components are being used and if they pose any risk to the organization.
- ✓ Integrates into your existing CI/CD pipeline to monitor every build for open source policy violations.
- ✓ Provides the most advanced remediation guidance to quickly resolve issues.



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).