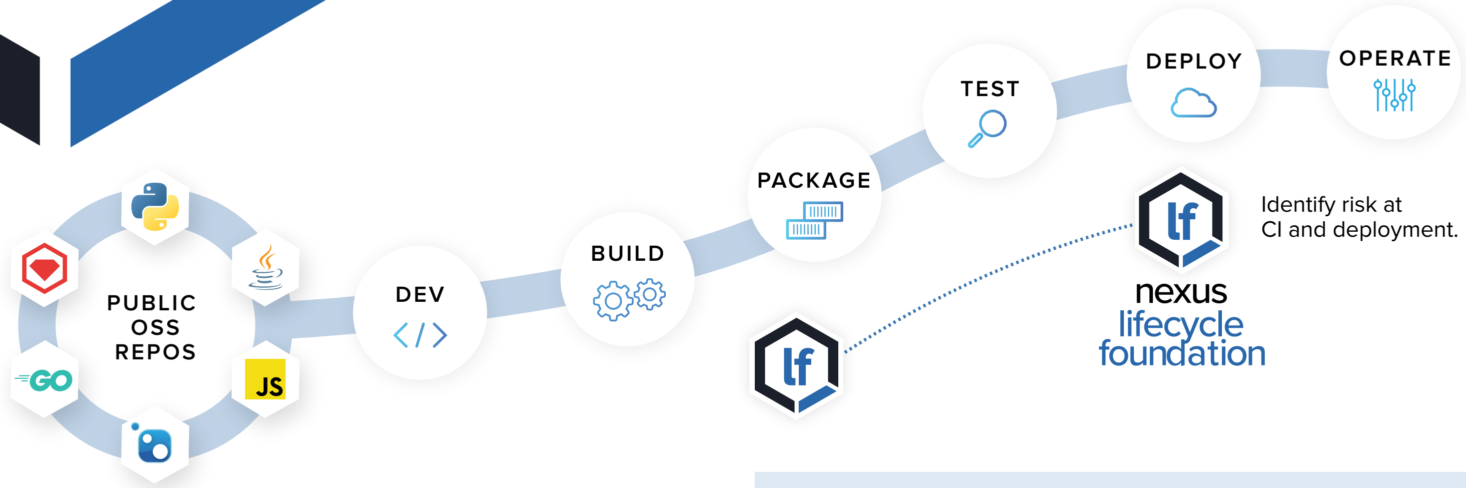
Nexus Lifecycle Foundation

Identify open source risk in your applications.

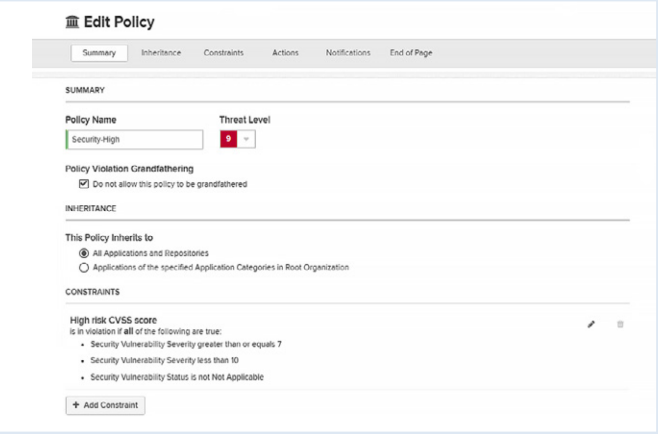
It's no secret. Developers use open source — in fact, 85% of a modern application is comprised of open source components, and unfortunately *one in ten* open source component downloads contain a known security vulnerability. Given this inherent risk, how do organizations ensure they are secure?

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.


PUBLIC OSS REPOS
GO
JS
DEV
BUILD
PACKAGE
TEST
DEPLOY
OPERATE
nexus lifecycle foundation
Identify risk at CI and deployment.

Create Customized Policies

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



Edit Policy

Summary | Inheritance | Constraints | Actions | Notifications | End of Page

SUMMARY

Policy Name: Security-High

Threat Level: 9

Policy Violation Grandfathering

☑ Do not allow this policy to be grandfathered

INHERITANCE

This Policy Inherits to

● All Applications and Repositories

○ Applications of the specified Application Categories in Root Organization

CONSTRAINTS

High risk CVSS score

is in violation if **all** of the following are true:

- Security Vulnerability Severity greater than or equals 7
- Security Vulnerability Severity less than 10
- Security Vulnerability Status is not Not Applicable

+ Add Constraint

SONATYPE NEXUS LIFECYCLE

#1 RANKED

SOFTWARE COMPOSITION ANALYSIS

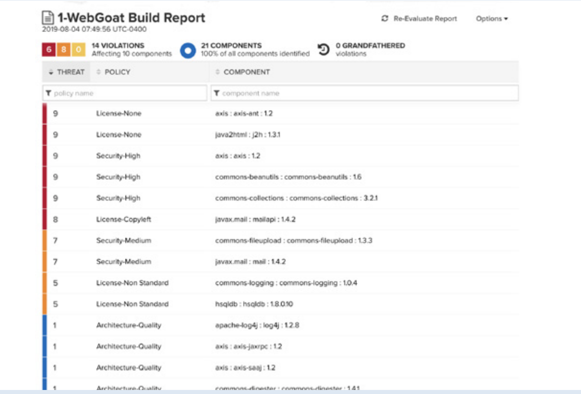
IT Central Station

> **"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



1-WebGoat Build Report
2019-08-04 07:49:56 UTC-0400

14 VIOLATIONS Affecting 10 components
21 COMPONENTS 100% of all components identified
0 GRANDFATHERED violations

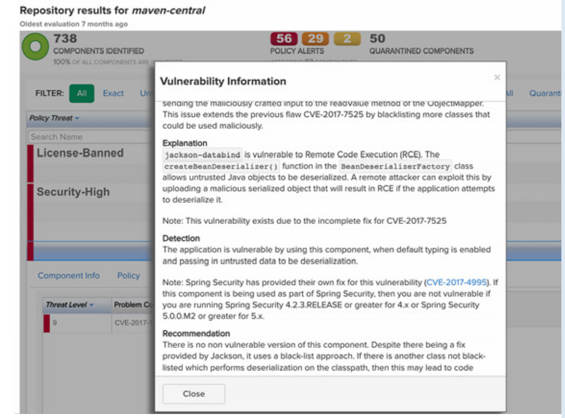
THREAT	POLICY	COMPONENT
9	License-None	axis : axis-ant : 1.2
9	License-None	java2html : j2h : 1.3.1
9	Security-High	axis : axis : 1.2
9	Security-High	commons-beanutils : commons-beanutils : 1.6
9	Security-High	commons-collections : commons-collections : 3.2.1
8	License-Copyleft	javax.mail : mailapi : 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 : 1.8.0.10
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

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.

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.



Repository results for *maven-central*
Oldest evaluation 7 months ago

738 COMPONENTS IDENTIFIED
100% OF ALL COMPONENTS ARE
56 29 2 POLICY ALERTS
50 QUARANTINED COMPONENTS

Vulnerability Information

sending 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.

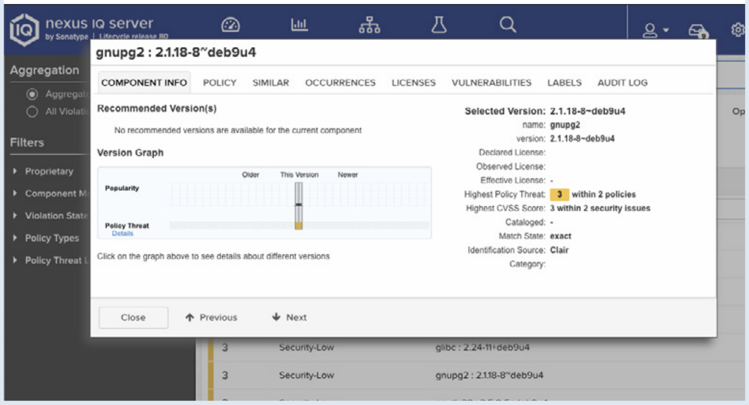
Explanation
`jackson-databind` is vulnerable to Remote Code Execution (RCE). The `createBeanDeserializer()` function in the `BeanDeserializerFactory` class allows untrusted Java objects to be deserialized. A remote attacker can exploit this by uploading a malicious serialized object that will result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



gnupg2 : 2.1.18-8~deb9u4

Recommended Version(s)

No recommended versions are available for the current component

Version Graph

Click on the graph above to see details about different versions

Selected Version: 2.1.18-8~deb9u4
name: gnupg2
version: 2.1.18-8~deb9u4
Declared License:
Observed License:
Effective License: -
Highest Policy Threat: 3 within 2 policies
Highest CVSS Score: 3 within 2 security issues
Cataloged: -
Match State: exact
Identification Source: Clair
Category:

3	Security-Low	glibc : 2.24-11+deb9u4
3	Security-Low	gnupg2 : 2.1.18-8~deb9u4

Identify and Fix Container Vulnerabilities

With integration to Red Hat Clair, you can view open source risk at all layers of the container (runtime, operating system, and application levels) within existing dashboards and reports. Use Nexus Lifecycle's flexible policy engine to govern open source risk within the entire container.

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.

sonatype

Sonatype is the leader in software supply chain automation technology with more than 300 employees, over 1,000 enterprise customers, and is trusted by over 10 million software developers. Sonatype's Nexus platform enables DevOps teams and developers to automatically integrate security at every stage of the modern development pipeline by combining in-depth component intelligence with real-time remediation guidance.

For more information, please visit **Sonatype.com**, or connect with us on **Facebook**, **Twitter**, or **LinkedIn**.