Nexus Auditor

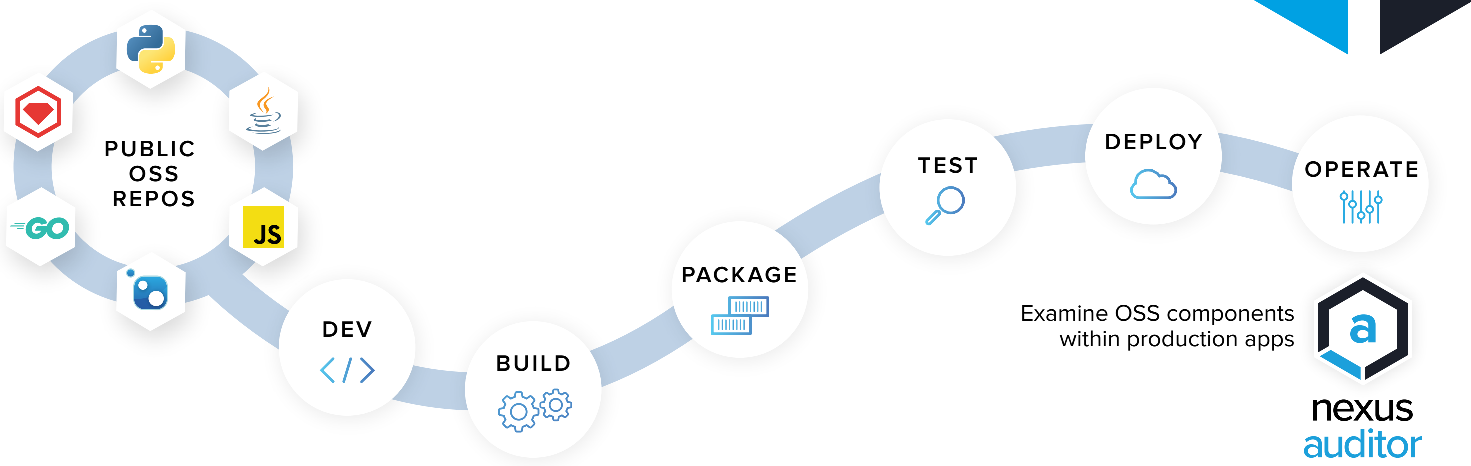
Monitor production and third-party apps for open source risk.

Open source components age more like milk than wine. With 1 in 10 open source component downloads containing a known security vulnerability, how do you manage risk in your production or third-party applications?

Organizations that outsource their development efforts to third parties must first understand what open source is included in those applications and if it poses any security or legal risk, before they put it in production.

Additionally, legacy applications no longer going through development must be analyzed to understand risk exposure relative to outdated open source components.

Manual verification methods don't scale. Visibility into open source usage is a requirement to mitigate risk.

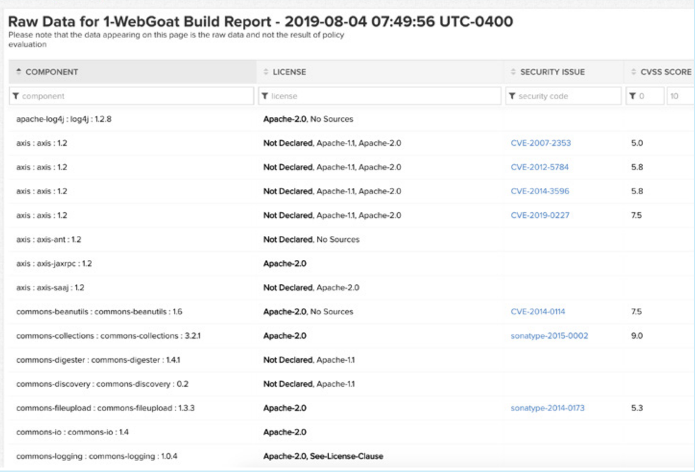


Examine OSS components within production apps

Generate a Software Bill of Materials

Nexus Auditor automatically generates a software bill of materials to identify open source components used within third-party or legacy applications.

Get a complete list of open source components included within your app to quickly identify components that violate your open source policies.



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

Please note that the data appearing on this page is the raw data and not the result of policy evaluation

COMPONENT	LICENSE	SECURITY ISSUE	CVSS SCORE
component	license	security code	0 10
apache-log4j : log4j : 1.2.8	**Apache-2.0**, No Sources		
axis : axis : 1.2	**Not Declared**, Apache-1.1, Apache-2.0	CVE-2007-2353	5.0
axis : axis : 1.2	**Not Declared**, Apache-1.1, Apache-2.0	CVE-2012-5784	5.8
axis : axis : 1.2	**Not Declared**, Apache-1.1, Apache-2.0	CVE-2014-3596	5.8
axis : axis : 1.2	**Not Declared**, Apache-1.1, Apache-2.0	CVE-2019-0227	7.5
axis : axis-ant : 1.2	**Not Declared**, No Sources		
axis : axis-jaxrpc : 1.2	**Apache-2.0**		
axis : axis-saaj : 1.2	**Not Declared**, Apache-2.0		
commons-beanutils : commons-beanutils : 1.6	**Apache-2.0**, No Sources	CVE-2014-0114	7.5
commons-collections : commons-collections : 3.2.1	**Apache-2.0**	sonatype-2015-0002	9.0
commons-digester : commons-digester : 1.4.1	**Not Declared**, Apache-1.1		
commons-discovery : commons-discovery : 0.2	**Not Declared**, Apache-1.1		
commons-fileupload : commons-fileupload : 1.3.3	**Apache-2.0**	sonatype-2014-0173	5.3
commons-io : commons-io : 1.4	**Apache-2.0**		
commons-logging : commons-logging : 1.0.4	**Apache-2.0, See-License-Clause**		

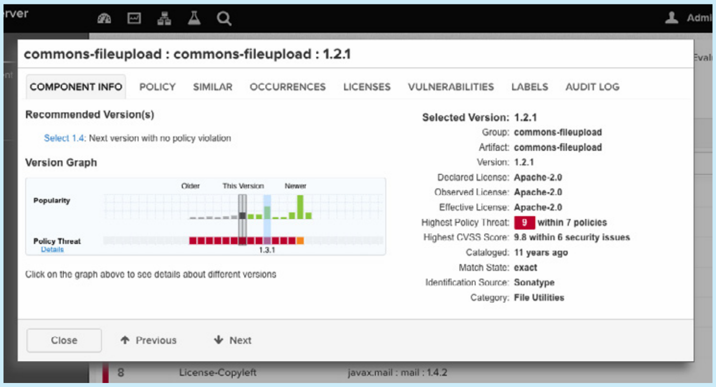
> "I would give this product a nine out of ten. I'll have a full report of artifacts—including those that are not secure—that would have been ingested into our organization. **That information is priceless.**
>
> —C. CHANI (FINANCIAL SERVICES),
> IT CENTRAL STATION REVIEW

www.sonatype.com

Triage License and Security Risk Within Third Party Applications

Before you accept an application from a third party, first scan it with Nexus Auditor to clearly see if any restricted licenses or security vulnerabilities exist.

With Auditor, you can analyze your inherent risk based on your open source policies and resolve issues with expert remediation guidance.



commons-fileupload : commons-fileupload : 1.2.1

Recommended Version(s)

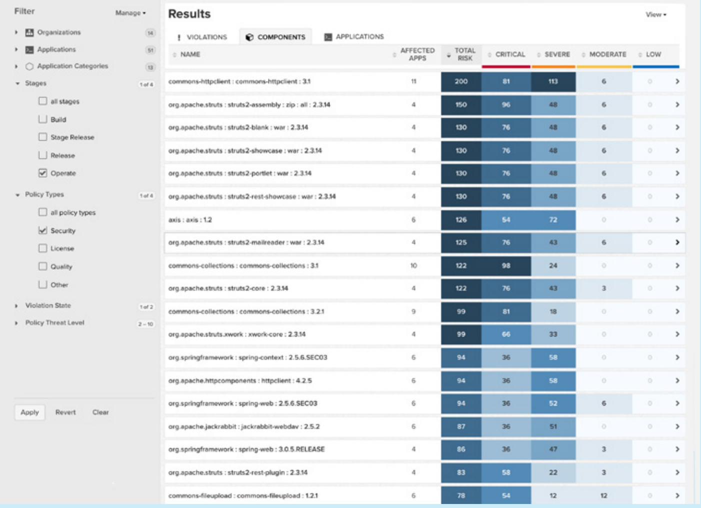
Select 1.4: Next version with no policy violation

Version Graph

Click on the graph above to see details about different versions

Selected Version: 1.2.1
Group: commons-fileupload
Artifact: commons-fileupload
Version: 1.2.1
Declared License: Apache-2.0
Observed License: Apache-2.0
Effective License: Apache-2.0
Highest Policy Threat: 9 within 7 policies
Highest CVSS Score: 9.8 within 6 security issues
Cataloged: 11 years ago
Match State: exact
Identification Source: Sonatype
Category: File Utilities

8 License-Copyleft javax.mail : mail : 1.4.2



Stages
- ☐ all stages
- ☐ Build
- ☐ Stage Release
- ☐ Release
- ☑ Operate

Policy Types
- ☐ all policy types
- ☑ Security
- ☐ License
- ☐ Quality
- ☐ Other

NAME	AFFECTED APPS	TOTAL RISK	CRITICAL	SEVERE	MODERATE	LOW
commons-httpclient : commons-httpclient : 3.1	11	200	81	113	6	0
org.apache.struts : struts2-assembly : zip : 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-portlet : 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	81	18	0	0
org.apache.struts.xwork : xwork-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
org.springframework : spring-web : 3.0.5.RELEASE	4	86	36	47	3	0
org.apache.struts : struts2-rest-plugin : 2.3.14	4	83	58	22	3	0
commons-fileupload : commons-fileupload : 1.2.1	6	78	54	12	12	0

Continuously Monitor Apps for New Vulnerabilities

An open source component might be free of security vulnerabilities today, but that doesn't mean it will stay that way forever. Nexus Auditor continuously monitors your production applications to identify newly disclosed vulnerabilities.

You'll receive an email or alert when a new vulnerability is found, so you can immediately take action to eliminate any threat from outside attackers.

Key Benefits of Nexus Auditor

✓ Protect third-party or legacy applications from vulnerable open source components.

✓ Continuously monitor applications for new risk and take action before it's too late.

✓ Feel confident that outsourced development teams are not using restrictive open source licenses, eliminating potential legal issues.

✓ Sleep better at night knowing that open source risk is being actively managed, even in applications no longer being developed.

> 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

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.**