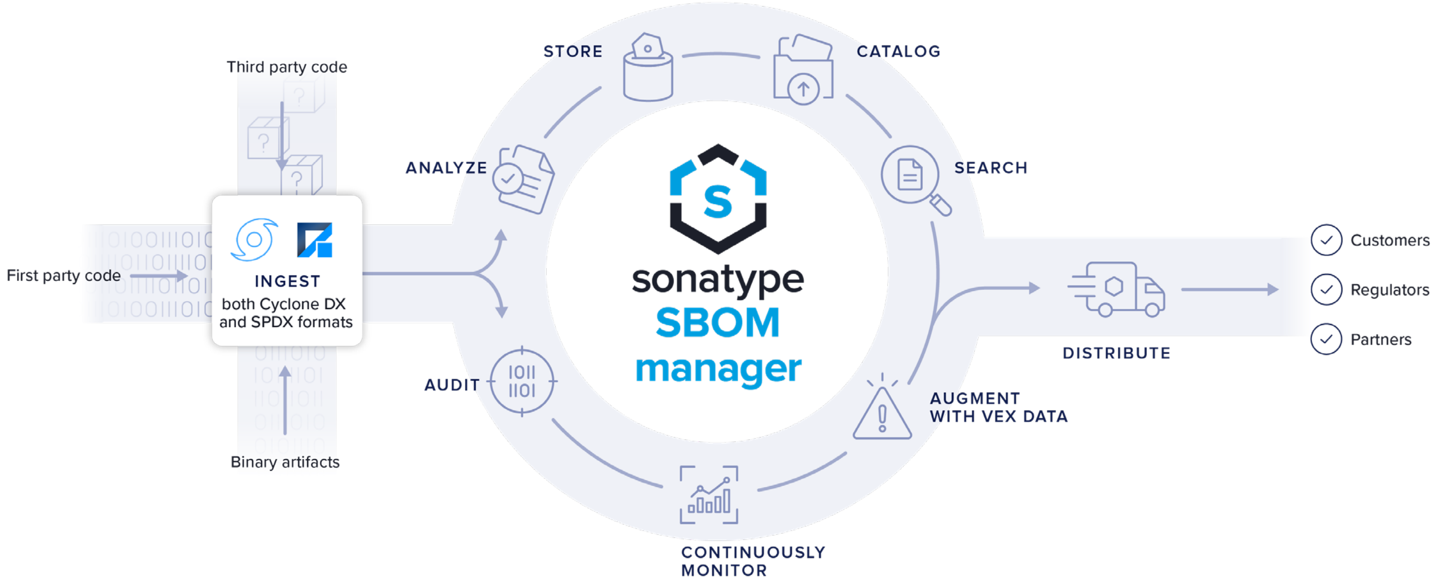
sonatype **SBOM manager**

Easy Compliance, Unlimited Scale.

Streamline and automate auditing, distributing, and monitoring SBOMs to achieve rapid, reliable compliance at scale. Your First and Third-party SBOMs – all in one place.

Reliably automate SBOM management at scale (1M+ SBOMs) from first and third-party sources.



Third party code

First party code

INGEST both Cyclone DX and SPDX formats

Binary artifacts

STORE

CATALOG

ANALYZE

SEARCH

sonatype SBOM manager

AUDIT

AUGMENT WITH VEX DATA

CONTINUOUSLY MONITOR

DISTRIBUTE

- ✓ Customers
- ✓ Regulators
- ✓ Partners

Sonatype knows SBOMs:

Regulations are here, making **SBOMs mandatory in 2024.**

Meet compliance standards by **sharing enriched SBOMs** at scale with automated VEX information and data that backs the world's #1 SCA tool.

FORRESTER®
WAVE LEADER 2023
Software Composition Analysis

Open Source Software is **full of risk.**

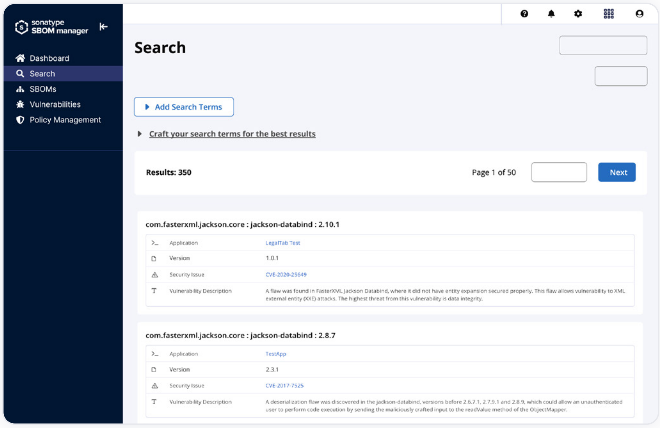
Continuously monitor first and third-party SBOMs for new security vulnerabilities, policy violations, and malware.

Sharing your software can put you in a **vulnerable position.**

The best companies trust Sonatype to understand their software contents and stay ahead of vulnerabilities so they can **build credibility with visibility.**

sonatype

Features



Search

Results: 350 Page 1 of 50

com.fasterxml.jackson.core : jackson-databind : 2.10.1

Application	LegalTab Test
Version	1.0.1
Security Issue	CVE-2020-25649
Vulnerability Description	A flaw was found in FasterXML Jackson Databind, where it did not have entity expansion secured properly. This flaw allows vulnerability to XML external entity (XXE) attacks. The highest threat from this vulnerability is data integrity.

com.fasterxml.jackson.core : jackson-databind : 2.8.7

Application	TestApp
Version	2.3.1
Security Issue	CVE-2017-7525
Vulnerability Description	A deserialization flaw was discovered in the jackson-databind, versions before 2.6.7.1, 2.7.9.1 and 2.8.9, which could allow an unauthenticated user to perform code execution by sending the maliciously crafted input to the readValue method of the ObjectMapper.

Audit SBOMs

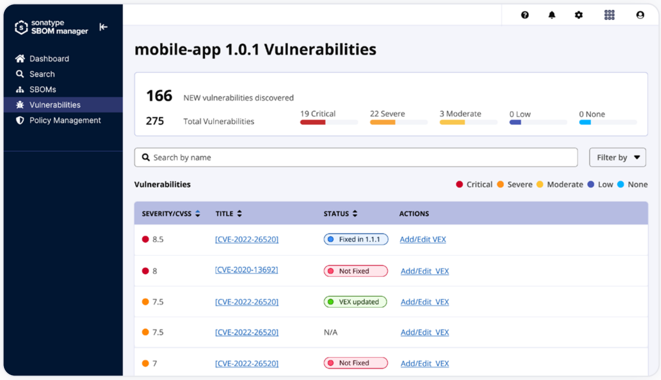
Simplify compliance, identify critical risks, and guide vendor negotiations with third-party software audit through SBOM Manager's smart and scalable database.

- **Catalog, Manage and Audit** SBOMs generated by you or a third party
- **Search** across all SBOMs to find components and vulnerabilities
- **Report** on application risk across every SBOM

Distribute SBOMs

Ensure regulatory compliance by sharing SBOMs at scale with automated Vulnerability Exchange information (VEX), keeping your customers and regulators informed and up-to-date.

- **Augment SBOMs** with VEX information to continuously update SBOMs with vulnerability and remediation data
- **Scale SBOM Approval** for new software versions by quickly applying VEX entries from previous versions
- **Distribute SBOMs via Vendor Porta**l to regulators, customers and partners



mobile-app 1.0.1 Vulnerabilities

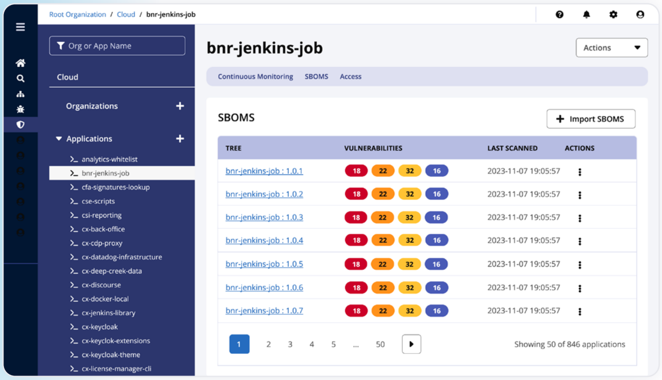
166 NEW vulnerabilities discovered

275 Total Vulnerabilities

19 Critical 22 Severe 3 Moderate 0 Low 0 None

Vulnerabilities

SEVERITY/CVSS	TITLE	STATUS	ACTIONS
● 8.5	[CVE-2022-26520]	Fixed in 1.1.1	Add/Edit VEX
● 8	[CVE-2020-13692]	Not Fixed	Add/Edit_VEX
● 7.5	[CVE-2022-26520]	VEX updated	Add/Edit_VEX
● 7.5	[CVE-2022-26520]	N/A	Add/Edit_VEX
● 7	[CVE-2022-26520]	Not Fixed	Add/Edit_VEX



bnr-jenkins-job

SBOMS

TREE	VULNERABILITIES	LAST SCANNED	ACTIONS
bnr-jenkins-job : 1.0.1	18 22 32 16	2023-11-07 19:05:57	⋮
bnr-jenkins-job : 1.0.2	18 22 32 16	2023-11-07 19:05:57	⋮
bnr-jenkins-job : 1.0.3	18 22 32 16	2023-11-07 19:05:57	⋮
bnr-jenkins-job : 1.0.4	18 22 32 16	2023-11-07 19:05:57	⋮
bnr-jenkins-job : 1.0.5	18 22 32 16	2023-11-07 19:05:57	⋮
bnr-jenkins-job : 1.0.6	18 22 32 16	2023-11-07 19:05:57	⋮
bnr-jenkins-job : 1.0.7	18 22 32 16	2023-11-07 19:05:57	⋮

Showing 50 of 846 applications

Continuously Monitor

Automatically monitor first and third-party SBOMs for new security vulnerabilities and malware risks. Respond promptly with the support of Sonatype's cutting-edge component intelligence.

- **Generate and Ingest** SBOMs from CycloneDX and SPDX format
- **Store** original and enriched SBOMs from first and third-party sources and meet retention requirements with historical version control
- **Analyze and Continuously Monitor** for vulnerabilities, malware, policy compliance, reduce patch response time for COTS and address issues before someone outside your organization does

sonatype

Sonatype is the software supply chain management company. We enable organizations to innovate faster in a highly competitive market. Our industry-leading platform empowers engineers to develop software fearlessly and focus on building products that power businesses. Sonatype researchers have analyzed more than 120 million open source components – 40x more than its competitors – and the Sonatype platform has automatically blocked over 115,000 malicious components from attacking software development pipelines. Enabling high-quality, secure software helps organizations meet their business needs and those of their customers and partners. More than 2,000 organizations, including 70% of the Fortune 100 and 15 million software developers, rely on our tools and guidance to be ambitious, move fast and do it securely. To learn more about Sonatype, please visit www.sonatype.com.