



Co-funded by
the European Union



OCCTET

Open Source Compliance Comprehensive tools and resources designed to simplify and streamline the CRA compliance process for SME, allowing them to tackle the complexities of OSS compliance.

Project Title: Open Source Compliance Comprehensive tools and resources designed to simplify and streamline the CRA compliance process for SME, allowing them to tackle the complexities of OSS compliance.

Project Acronym: OCCTET

Grant Agreement / Contract No.: 101190474

Program: DIGITAL Europe Programme; DIGITAL-ECCC-2024-DEPLOY-CYBER-06

Instrument: DIGITAL JU SME Support Action

Granting Authority: European Cybersecurity Industrial, Technology and Research Competence Centre

Project Start Date: 1 November 2024

Project Duration: 24 months

Deliverable Number: D 3.3

Deliverable Title: Toolkit-Demo-Del

Deliverable Type (DOA): DEM - Demonstrator, pilot, prototype

Deliverable Type (content): Report & Methodology (including Software Tool Description)

Work Package: WP3 – Build Open Source Tools to Automate Evaluation

Dissemination Level: PU – Public

Due Date (DoA): 31 March 2026

Actual Submission Date: 31 May 2026

Version: 1.1

Lead Beneficiary: BS - Bitsea

Main Author(s): Hans-Juergen Schumacher - BS; Sebastian Schuberth – DO, Philippe Ombredanne - ABCD

Contributing Partner(s): ECL, DO, BS, ABCD

Reviewer: ECL - Eclipse Foundation Europe

Licensing (public Deliverable)

This deliverable is licensed under: CC-BY 4.0 (Attribution 4.0 International)

Source code of the CRA Self-Assessment Platform is available at:

<https://github.com/expertware/OCCTET-CRA-self-assessment>

Legal Notice

This deliverable has been produced within the OCCTET project (Grant Agreement No. 101190474) funded under the Digital Europe Programme.

Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.



Document History

Version	Date	Issued By	Status	Comments
0.1	16-03-2026	BS	Draft	Initial draft of D3.3
1.0	31-03-2026	ECL	Release	Review document and release
1.1	31-05-2026	ECL	Release	Extension of SME data and OSS projects



Executive Summary

Overview and Strategic Context This document presents the findings and progress of Deliverable D3.3 (Toolkit-Demo-Del) developed under Work Package 3 of the OCCTET (Open Source Compliance Comprehensive Tools and Efforts for Trustworthiness) project. Funded under the DIGITAL Europe Programme, OCCTET addresses the critical need for European Small and Medium-sized Enterprises (SMEs) to manage open-source software (OSS) compliance. The toolkit specifically mitigates the regulatory and operational burdens introduced by the Cyber Resilience Act (CRA), which mandates strict vulnerability management and "security by design" for products with digital elements.

Core Objectives

The primary objectives realized in this demonstrator phase include:

- Developing an open-source toolkit to streamline the generation of Software Bill of Materials (SBOMs) to catalogue software components efficiently.
- Implementing automated evaluation mechanisms for swift vulnerability detection and severity prioritization.
- Automating compliance reporting by generating critical artifacts, including SBOMs and Vulnerability Exploitability eXchange (VEX) documents, to simplify adherence to CRA standards.

Technical Architecture and Toolchain

The OCCTET toolchain integrates advanced, open-source compliance platforms designed for scalability and precision:

- **ORT Server (Double Open Compliance - DOC):** Acting as the foundational platform, the ORT Server leverages the OSS Review Toolkit to perform deep, dynamic Software Composition Analysis (SCA) without requiring modifications to the analyzed projects. It features a comprehensive REST API and a React-based web frontend for managing user access, product hierarchies, and vulnerability dashboards. The ORT Server automates dependency discovery, license scanning, and continuous vulnerability monitoring via schedule-triggered workflows.
- **OCCTET Curator:** An AI-supported, microservices-based web application tailored for audit curation and metadata enrichment. The Curator integrates local Large Language Models (LLMs) to automate intelligent text analysis, false positive detection, and license classification without exposing sensitive data to external cloud APIs. It processes scanner results to generate highly accurate, CRA-aligned SBOMs (SPDX and CycloneDX formats) and structured VEX documents to communicate exact exploitability statuses.

Validation and Testing

The toolkit demonstrator has undergone robust testing utilizing diverse data sets:



-
- Validation targets include widely used open-source infrastructure projects (e.g., Apache Kafka, Hadoop, Tomcat, Jetty) and specific SME use cases (e.g., ReductStore).
 - Testing confirms the toolkit's capability to analyze complex dependencies, flag technical issues, and continuously track evolving security vulnerabilities over time.

Future Outlook

The OCCTET toolchain is progressing according to schedule, demonstrating a strong outlook for sustained usage beyond the project lifecycle due to its open-source licensing model. Under the current development plan, efforts will continue within Work Package 3 to deliver an up-to-date version of the toolkit by May 31, 2026. This upcoming release aims to incorporate a broader range of SME use cases to further validate the system's efficacy. However, it must be highlighted that securing active SME involvement for the testing and validation processes within Work Package 4 has proven to be a significant challenge. Despite these difficulties in engagement, outreach efforts remain a priority to gather the necessary feedback. This feedback will drive planned enhancements such as extended repository support, refined vulnerability resolution mappings tailored to CRA requirements, and optimized OpenVEX reporting culminating in the delivery of the final, fully featured toolkit by October 31, 2026.



Table of contents

1 Context	12
1.1 Grant agreement	12
1.2 OCCTET outlook for end of the project, 31.10.2026	12
1.3 Background	13
1.4 What are SBOMs	14
1.4.1 Security and Vulnerability Management	15
1.4.2 Supply Chain Transparency and Due Diligence	16
1.4.3 License Compliance	16
1.5 SBOM and CRA	16
1.5.1 Supporting security updates and patch management	16
1.5.2 Compliance with vulnerability disclosure requirements	17
1.5.3 Enabling lifecycle risk management	17
1.5.4 VEX – supplement to the SBOM in the context of cybersecurity and ICT risk management	17
1.5.5 Beyond Security: SBOMs Must Also Address Licensing Obligations	18
2 Introduction	19
2.1 Toolchain	19
2.2 Testdata	19
2.2.1 Open Source Projects	19
2.2.2 SME	20
3 ORT Server (DOC)	21
3.1 Double Open's Role in OCCTET	21
3.2 Architectural Overview	21
3.3 CRA Phases	23
3.4 Vulnerability Management	23
3.5 Dependency Management	30
3.6 SBOM Generation	32
3.7 ORT Dependency and Vulnerability Analysis of Popular Open Source Projects	33
3.7.1 Popular Open Source Projects	33
3.7.1.1 Introduction	33
3.7.1.2 Overall Summary	34
C/C++ Projects	35
boostorg/boost	35
curl/curl	35
ffmpeg/ffmpeg	35
gabime/spdlog	35
madler/zlib	35
opencv/opencv	35
open-source-parsers/jsoncpp	35



openssl/openssl	35
protocolbuffers/protobuf	35
qt/qtbase	35
C# Projects	35
App-vNext/Polly	35
AutoMapper/AutoMapper	35
AvaloniaUI/Avalonia	35
DapperLib/Dapper	35
dotnet/runtime	35
FluentValidation/FluentValidation	35
JamesNK/Newtonsoft.Json	35
NLog/NLog	35
restsharp/RestSharp	35
serilog/serilog	35
Swift Projects	36
Alamofire/Alamofire	36
Kitura/Kitura	36
Moya/Moya	36
mxcl/PromiseKit	36
onevcats/Kingfisher	36
PerfectlySoft/Perfect	36
ReactiveX/RxSwift	36
SnapKit/SnapKit	36
SwiftyJSON/SwiftyJSON	36
vapor/vapor	36
Rust Projects	36
BurntSushi/memchr	36
cuviper/autocfg	36
dtolnay/proc-macro2	36
dtolnay/quote	36
dtolnay/unicode-ident	36
matklad/once_cell	36
microsoft/windows-rs	36
rust-lang/cfg-if	36
rust-lang/libc	36
rust-lang/log	36
Ruby Projects	36
Repository	36
guard/guard	36
jnunemaker/httparty	36
lostisland/faraday	36



rack/rack	36
rails/rails	36
rails/thor	36
rest-client/rest-client	36
ruby/json	36
sparklemotion/nokogiri	36
sparklemotion/sqlite3-ruby	36
Python Projects	37
Repository	37
benjaminp/six	37
certifi/python-certifi	37
dateutil/dateutil	37
jawah/charset_normalizer	37
kjd/idna	37
numpy/numpy	37
psf/requests	37
pypa/packaging	37
python/typing_extensions	37
urllib3/urllib3	37
Go Projects	37
davecgh/go-spew	37
go-yaml/yaml	37
modern-go/concurrent	37
modern-go/reflect2	37
pkg/errors	37
pmezard/go-difflib	37
spf13/pflag	37
stretchr/testify	37
golang.org/x/text	37
PHP Projects	37
doctrine/dbal	37
doctrine/orm	37
guzzle/guzzle	37
laravel/framework	37
php-fig/log	37
Seldaek/monolog	37
symfony/console	37
symfony/dependency-injection	37
symfony/yaml	37
twigphp/Twig	37
JavaScript Projects	37



feross/safe-buffer	38
inspect-js/hasOwn	38
isaacs/inherits	38
isaacs/node-graceful-fs	38
ljharb/has-symbols	38
lydell/js-tokens	38
microsoft/tslib	38
npm/wrappy	38
Raynos/function-bind	38
TooTallNate/util-deprecate	38
JVM Projects	38
external/jsr-305	38
apache/commons-logging	38
apache/commons-collections	38
eclipse-ee4j/injection-api	38
google/guava	38
JetBrains/java-annotations	38
qos-ch/slf4j	38
3.7.1.3 Vulnerability Findings	38
3.7.1.4 Top 5 Repositories by Vulnerability Count	39
mxcl/PromiseKit	39
Example 2 UI view:	40
boostorg/boost	40
openssl/openssl	41
qt/qtbase	42
rails/rails	43
3.7.2 Renowned Open Source Projects	43
3.7.2.1 Hadoop	43
3.7.2.2 Kafka	44
3.7.2.3 Tomcat	45
3.7.2.4 Mosquitto	45
3.7.2.5 Jetty	46
3.8 Planned Improvements	46
4 Curator	48
4.1 Bitsea's role in OCCTET	48
4.2 OCCTET Curator On GitHub	48
4.3 Current Status	48
4.4 Installation	49
4.5 Architecture	49
4.6 User Interface	49
4.7 Microservices and Task Isolation	50



4.8 Messaging Infrastructure: NATS and JetStream	50
4.9 AI and Local Language Model Integration	51
4.10 External Data Sources and Enrichment	51
4.11 Open Source Licensing and Sustainability	51
4.12 Deployment and Packaging	51
4.13 Docker images	52
4.14 Vulnerability Detection and CRA Alignment	52
4.15 VEX integration	53
4.16 Validation with SME data	53
4.16.1 SME-Tester: ReductSoftware UG	53
4.16.2 SME Tester: Obeo	58
4.17 Validation with OSS projects	58
4.17.1 projects	58
4.17.1.1 dotnet/runtime	58
4.17.1.2 Avalonia	61
4.17.1.3 Newtonsoft.Json	63
4.17.1.4 Polly	64
4.17.1.5 Restsharp	66
4.17.1.6 Dapper	68
4.17.1.7 Fluent validation	70
4.17.1.8 Automapper	72
4.17.1.9 Serilog	73
4.17.1.10 NLog:	75
4.17.2 Iconic Projects	76
4.17.2.1 Adoptium	76
4.17.2.2 Eclipse IDE	77
4.17.2.3 Eclipse Mosquitto	80
4.17.2.4 Tomcat	82
4.17.2.5 Kafka	83
4.17.3 Python projects	85
4.17.3.1 Type-extensions 4.13.2	85
4.17.3.2 idna -3.10.0	86
4.17.3.3 Certifi 2025.4.26	88
4.17.3.4 Six-1.17.0	89
4.17.3.5 Charset-normalizer-3.4.1	91
4.17.3.6 Requests-2.32.3	93
4.17.3.7 Urllib3-2.4.0	96
4.17.3.8 Python-dateutil-2.9.0.post0	98
4.17.3.9 Numpy-2.2.5	101
4.17.3.10 Packaging-25.0	103
4.17.4 Swift projects	104



4.17.4.1 Alamofire	104
4.17.4.2 Vapor	106
4.17.4.3 ReactiveX	108
4.17.4.4 Kingfisher	111
4.17.4.5 SwiftyJSON	114
4.17.4.6 Snapkit	115
4.17.4.7 Moya	116
4.17.4.8 Promisekit	118
4.17.4.9 Perfect	121
4.17.4.10 Kitura	123
4.17.5 Go projects	125
4.17.5.1 errors 0.9.1	125
4.17.5.2 Go_spew	126
4.17.5.3 Go-yaml-3.0.1	127
4.17.5.4 Modern-go-concurrent	128
4.17.5.5 Modern-go-reflect2	129
4.17.5.6 Pflag-1.0.5	130
4.17.5.7 Pmezard-go-difflib	130
4.17.5.8 Stretchr_testify	131
4.17.5.9 Text-0.21.0	133
4.17.5.10 Yaml-2.4.0	134
4.17.6 Ruby Projects	135
4.17.6.1 Rails	135
4.17.6.2 Nokogiri	138
4.17.6.3 Ruby/JSON	141
4.17.6.4 Httparty	143
4.17.6.5 Faraday	145
4.17.6.6 Guard	148
4.17.6.7 Thor	150
4.17.6.8 Rest-client	152
4.17.6.9 Rack	156
4.17.6.10 Sqlite3-ruby	158
4.17.7 JVM projects	160
4.17.7.1 Annotations 13.0	160
4.17.7.2 Com.google.code.findbugsjsr305-3.0.2	161
4.17.7.3 Listenablefuture-9999.0.empty-to-avoid-conflict-with-guava	162
4.17.7.4 Commons-logging-1.2	163
4.17.7.5 Guava-failureaccess-1.0.1	164
4.17.7.6 Javax-inject-1	165
4.17.7.7 Org.slf4j-api-1.7.25	166
4.17.7.8 aopalliance -1.0	167



4.17.7.9 Org-slf4j-api	168
4.17.7.10 Commons-collections 3.2.2	168
4.17.8 Javascript/Typescript projects	169
4.17.8.1 Tslib-2.8.1	169
4.17.8.2 Inherits-2.0.4	170
4.17.8.3 Function-bind-1.1.2	171
4.17.8.4 Hasown-2.0.2	172
4.17.8.5 Js-tokens-4.0.0	172
4.17.8.6 Safe-buffer-5.2.1	173
4.17.8.7 Util-deprecate-1.0.2	174
4.17.8.8 Has-symbols-1.1.0	175
4.17.8.9 Wrappy-1.0.20	175
4.17.9 Eclipse Projects	176
4.17.9.1 Eclipse-Mosquitto 2.1.2	176
4.17.9.2 Hadoop 3.4.1	178
4.18 Conclusion	180
5 Conclusions	182
6 ACRONYMS AND ABBREVIATION	183
7 BIBLIOGRAPHY	184



1 Context

This section describes the requirements for the deliverables in the OCCTET project and their fulfilment at different stages of the project.

1.1 Grant agreement

As per the grant agreement, the objectives of this Work Package 3 are as follow:

- Develop an open source toolkit to streamline the generation of SBOMs, facilitating the efficient identification and cataloguing of software components within digital assets.
- Implement automated evaluation mechanisms to swiftly assess software vulnerabilities, enabling prompt detection and prioritisation based on their severity and potential impact.
- Enable effective remediation strategies by offering actionable insights and recommendations to address software vulnerabilities through patch management, version updates, and configuration adjustments.
- Assess the security posture of open source components, evaluating their security practices, exposure to known vulnerabilities, and overall maintenance status to ensure the use of secure components in software development.
- Automate compliance reporting with the generation of critical documents such as SBOMs and Vulnerability Exploitability Exchange (VEX) documents, aiding in adherence to Critical Risk Assessment (CRA) standards and simplifying regulatory compliance processes.

As per the Grant agreement, the delivery 3.3 in the whole OCCET project is as follows:

- Demonstrator of the toolkit on use cases from WP4

As per the Grant agreement, the remaining deliverables under Work Package 3:

Deliverable D3.4 FedDB-Final-Del WP3

Primary partner: ABCD

Description: Demonstrator, pilot, prototype

Dissemination level: Public

At the end of month 17 (31.5.2026) (Extended Time)

The final version of the toolkit is to be delivered under Work Package 4, as D4.1, by 31.10.2026.

1.2 OCCTET outlook for end of the project, 31.10.2026

The toolchain solution has progressed as planned, and concurrent improvements alongside the project have further supported the project, extending and benefiting the results of the project. The decision to use open source licensed tooling has clearly been proven, as concurrent improvements done by others than the project itself, benefit also the project



results, all being part of the same open source projects. There is a great outlook for the usage of the tooling solution also after the project, considering the interest and usage not only by project participants but also non-project parties.

The project is now in the phase of testing the tooling, mainly happening under Work Package 4, and incrementally improving the tooling based on the results of the testing. We are seeing signals of both organic adoption from iconic open source projects as well as adoption from SMEs due to OCCTET project outreach. OCCTET project outreach has helped us understand potential areas for improvement, and that work will continue as part of the testing part of the project.

The fact that the OCCTET tooling is open source, and developed as an open source project, has ensured and will continue to ensure the long-term utility and availability of the results of the project. However, the practical validation of these tools remains constrained by the significant and ongoing difficulty of identifying SMEs that are willing and available to actively participate as testers.

1.3 Background

In today's interconnected digital economy, Free and Open Source Software (FOSS) forms the invisible backbone of nearly every product with digital elements. From routers and medical devices to mobile apps and enterprise platforms, developers across all sectors routinely rely on FOSS to accelerate development, reduce costs, and foster innovation. It is estimated that between 90% to 99% of modern software products incorporate open source components making FOSS not only ubiquitous but mission-critical to Europe's digital infrastructure.

However, this widespread dependence on FOSS also exposes systemic vulnerabilities. Security incidents such as the Log4Shell vulnerability and the recent XZ Utils backdoor have highlighted how a single flaw in a widely used open source library can cascade through thousands of products across sectors. More recently, high-profile software supply chain attacks such as the s1ngularity malware embedded in the Nx npm package, or the NPM supply chain attack on popular packages like chalk and debug have exposed how a single compromised component can cascade across thousands of downstream applications. Moreover, many companies, especially Small and Medium-sized Enterprises (SMEs) are unaware of the full extent of their open source dependencies, let alone how to manage their compliance and cybersecurity risks.

Amid growing cyber threats, the EU must increasingly treat open source base technologies as digital infrastructure. Securing open source software means securing the foundation of all our digital systems. As noted in the EU Sovereign Tech Fund Feasibility Study, the scale of this need is vast because open source code is integral to nearly every digital asset. Its open nature enables innovation, but it also requires deliberate security and maintenance strategies. Like water management systems or transport networks, open source software must be maintained with public investment because failures can have cascading consequences.

FOSS plays a role comparable to roads and bridges in physical infrastructure, capital markets in economic systems, and water in environmental systems. In each of these analogies, open source code forms a critical enabler — and its maintenance offers high-return investment. According to the Linux Foundation, 70–90% of modern software stacks are composed of open source code. Replacing this would cost the European



economy an estimated €8.8 trillion — underscoring FOSS not just as a technical asset but a pillar of Europe’s economic independence, innovation, and competitiveness.

Recognizing these challenges, the European Union has introduced landmark legislation such as the Cyber Resilience Act (CRA) and the NIS2 Directive, which impose strict obligations on manufacturers to ensure that digital products including the third-party components they incorporate — meet essential cybersecurity and documentation requirements. Notably, Article 10(4) of the CRA states that manufacturers must ensure all integrated software, including FOSS, does not compromise the product’s cybersecurity. The Cyber Resilience Act (CRA) represents a landmark shift in the European Union’s approach to cybersecurity. By introducing mandatory cybersecurity and vulnerability management obligations for manufacturers of digital products and software, the CRA establishes a horizontal legal framework that directly affects the development and distribution of nearly all products with digital elements (PDEs) in the EU internal market. This includes not only hardware devices but also general-purpose and embedded software components.

The CRA is grounded in the principle that cybersecurity must be embedded “by design” throughout the product lifecycle—from development to deployment and post-market surveillance. This introduces new obligations such as vulnerability reporting, technical documentation, secure update mechanisms, and clear communication with end-users. In particular, Annex I and Article 10 of the CRA emphasize transparency, secure software development practices, and detailed technical documentation of software components and known vulnerabilities.

While these legal developments are crucial for improving digital trust, they pose practical difficulties for SMEs. Without dedicated legal or compliance teams, many SMEs struggle to verify software origins, fulfill license obligations, or track vulnerabilities across their dependency trees. Manual compliance processes are time-consuming and costly, creating a compliance gap that threatens to leave smaller actors behind.

The OCCTET Project (**Open-source Compliance: Comprehensive Techniques and Essential Tools**) was created to directly address this gap. Co-funded by the European Commission through the Digital Europe Programme, OCCTET is a strategic initiative designed to equip European SMEs with robust, user-friendly, and freely available tools to manage open source compliance and meet regulatory expectations. The project aims to significantly lower the costs for CRA compliance by automating key processes such as Software Bill of Materials (SBOM) generation, license verification, and vulnerability management.

This report provides a comprehensive update on the project's rationale, objectives, technical work packages, SME-oriented use cases, ongoing development, and future deliverables.

1.4 What are SBOMs

As Open Source Software is a regular component of software, from consumer goods to security-relevant systems at the national level, the Software Bill of Materials (SBOM) has established itself as a key tool for meeting legal and security requirements.¹ Similar to the

¹ In both the US and the EU, SBOMs are promoted as a key security tool through policy requirements. In the US, Executive Order 14028 mandates SBOMs for government software, accompanied by NTIA standards and CISA implementation measures. In the EU, the Cyber Resilience Act provides for transparency regarding software components; on August 4, the Federal Office for Information Security (BSI) published Part 2 of Technical Guideline TR-03183 "Cyber Resilience Requirements." Software bills of materials (SBOMs) are



classic bill of materials in the manufacturing industry, the SBOM documents all components – especially third-party components of a software application in a structured form.² The SBOM is typically a directory of software components that can be read by both humans and machines, including associated metadata (e.g., name, version, manufacturer, and license type).

Against the backdrop of today's highly component-based software development, many products are based on a large number of open source libraries and third-party components, whose development and maintenance status can change significantly over time. For example, components may become obsolete, vulnerable to security risks, functionally inadequately documented, or without active maintenance by the community. In such cases, there is an increased risk of operational failures or significant additional costs for the maintenance and further development of the software in question.³

Such risks are particularly relevant for regulated industries (e.g., medical devices, aviation technology), for products with long operating or maintenance cycles (such as industrial control systems or safety-critical infrastructures), and in areas with special requirements for reliability and traceability. In these contexts, unstable or no longer available components can significantly impair compliance with industry-specific regulations, operational safety, and maintainability.

A continuously maintained and structured SBOM can be used to identify at an early stage which components are classified as risky in this respect. This makes it possible to proactively implement countermeasures such as refactoring, component replacement, or support contracts, thereby ensuring the long-term operability of the software product.

SBOMs serve three primary legal and operational purposes that are now widely recognized across both public procurement and private sector software development:

1.4.1 Security and Vulnerability Management

The modern SBOM has expanded beyond compliance to address operational and national security concerns. As Dirk Riehle notes, "to manage operational risk, you need to understand what components are doing their job and whether new vulnerabilities have been discovered". This shift is also reflected in regulatory instruments like the U.S. Executive Order 14028 and the CRA, which make SBOMs a legal requirement for vulnerability tracking and response. To complement this, the ISO/IEC DIS 18974:2023 standard specifies the role of SBOMs as an integral part of a structured, security-oriented software development and maintenance process and as a basis for performing risk analyses and implementing effective measures within the framework of the Secure Software Development Life Cycle (SSDLC).

among the key requirements of the European Cyber Resilience Act (CRA). Software bills of materials (SBOMs) are among the key requirements of the European Cyber Resilience Act (CRA).

<https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/TR-03183-2-SBOM-Anforderungen.html>, 23/09/ 2025

²D. Riehle, "The Software Bill of Materials" in Computer, vol. 58, no. 04, pp. 115-120, April 2025, <https://www.computer.org/csdl/magazine/co/2025/04/10938013/25mYHqTDkZO>

³OWASP Top 10 Risks for Open Source Software <https://owasp.org/www-project-open-source-software-top-10/> accessed on 23/09/2025



1.4.2 Supply Chain Transparency and Due Diligence

SBOMs now feature prominently in commercial contractual diligence, such as vendor assessments and M&A transactions. Customers frequently require SBOMs as part of software procurement contracts, particularly to review license compliance or identify potential exposure to restrictive terms (e.g., GPL copyleft clauses). Heather J. Meeker emphasizes that due diligence must include audits of embedded third-party code and license documentation. OpenChain's compliance framework reflects this in its emphasis on supplier-side transparency and documentation for inbound and outbound OSS use.

Moreover, due to the sheer scale of indirect dependencies (often comprising over 90% of the total code base), most risk lies in components developers may not even be aware of. This reinforces the need for robust SBOM practices throughout the development and delivery lifecycle.

1.4.3 License Compliance

An SBOM provides the foundation for determining which licenses apply to a software product's components. This is critical for satisfying attribution obligations, fulfilling source code access requirements under copyleft licenses, and avoiding inadvertent license violations. As Heather J. Meeker emphasizes, tracking open source usage is essential to mitigate copyright risks and provide required notices to downstream users. This is also codified in ISO/IEC 5230:2020 (OpenChain Specification) which mandates a clearly defined process for identifying OSS components and their license obligations.

1.5 SBOM and CRA

The CRA requires hardware and software manufacturers to implement a series of cybersecurity measures based on the principle of "security by design." This principle requires that security aspects be taken into account at the earliest stages of product development. In addition, manufacturers are required to provide security updates throughout the entire life cycle of a product and to remedy known vulnerabilities promptly and effectively. Violation of these obligations can result in significant legal consequences, including fines, recalls, or restrictions on market access within the EU. Article 3(39) of the CRA introduces a legally binding definition of the term "software bill of materials" (SBOM): "Software bill of materials" means a formal record of the details and supply chain relationships of the components contained in the software elements of a product with digital elements;"

This explicitly qualifies the SBOM as a legally relevant artifact necessary for fulfilling regulatory obligations in the area of cybersecurity and not merely as a best practice. According to the CRA, SBOMs are an important tool for fulfilling explicit regulatory obligations related to risk management, vulnerability handling, and update requirements. An SBOM under the CRA is a means to an end, not the end itself.

1.5.1 Supporting security updates and patch management

The CRA requires manufacturers to provide security updates throughout the entire period during which a product is marketed or supported. A complete and accurate SBOM enables development and security teams to identify precisely those components that need to be updated or patched as soon as new vulnerabilities become publicly known, especially in complex dependency chains.



1.5.2 Compliance with vulnerability disclosure requirements

Articles 13 and 14 of the CRA require manufacturers to establish procedures for coordinated vulnerability disclosure. An SBOM improves the manufacturer's ability to respond to reported vulnerabilities in a legally compliant and efficient manner by clearly identifying which components may be affected and whether affected software versions have already been shipped.

1.5.3 Enabling lifecycle risk management

Annex I Part II of the CRA establishes a direct link between SBOMs and risk management procedures. Manufacturers are required to continuously identify security risks, assess them, and implement appropriate risk mitigation measures. The SBOM provides the factual basis for risk analysis by disclosing exactly which software components including open source and transitive dependencies have been used.

However, an SBOM alone is not sufficient to meet the requirements of the CRA. The regulation requires active risk management, which includes the following steps:

- Knowledge of the components used
- Identifying known vulnerabilities in these components,
- Implementation of appropriate remedial measures.

Risk management therefore requires transparency about software components. Only those who know which components are contained in the software can assess the extent to which known security vulnerabilities pose a concrete threat. While this is often traceable in commercial third-party libraries through contractually regulated license and update conditions, dealing with open-source components requires proactive and documented recording. This documentation is provided by the SBOM and thus forms the backbone of all further compliance measures.

1.5.4 VEX – supplement to the SBOM in the context of cybersecurity and ICT risk management

The SBOM provides a structured list of all components of a software product. It provides transparency about the components used, but does not provide any immediate information about whether known vulnerabilities in these components can actually be exploited in the respective application or operating environment. This is where the Vulnerability Exploitability eXchange (VEX) specification comes into play. A VEX document supplements the SBOM with machine-readable information on whether certain vulnerabilities affect the product in its actual delivered state. This enables manufacturers, users, and operators to set priorities for security measures in a targeted manner while avoiding unnecessary or risk-free patches. The integration of VEX documents into SBOMs has established itself as a best practice and is supported internationally by various stakeholders. The machine-readable linking of component information with the exploitability status of known vulnerabilities contributes significantly to increased efficiency and automation in security-related processes.

The US Cybersecurity and Infrastructure Security Agency (CISA) has emphasized the importance of VEX integration in several publications, particularly for promoting the automated and effective use of SBOMs. A study published in 2025 also shows that adding vulnerability status in VEX format to SBOMs significantly increases the practical usefulness of these tools, especially for maintenance and security teams. While the authors cite



challenges in standardization and automation, they also demonstrate the potential of VEX for continuous, machine-readable tracking of security risks²²

1.5.5 Beyond Security: SBOMs Must Also Address Licensing Obligations

While the CRA emphasizes the role of SBOMs primarily in the context of vulnerability tracking, risk mitigation, and security updates, this focus reflects only one dimension of SBOM utility. In practice, a complete and correct SBOM also captures the legal metadata associated with each component and most importantly, the license(s) under which it is used.

This broader interpretation is not only rooted in industry practice (as defined by standards such as SPDX, CycloneDX, and OpenChain ISO/IEC 5230) but is also essential to fulfill other legal and contractual obligations, including:

- License attribution and notice compliance
- Copyleft license obligations, including source code disclosure triggers
- Commercial and IP due diligence in vendor, customer, and M&A contexts

In short, license compliance and vulnerability management are two sides of the same SBOM coin.

From a compliance and operational standpoint, this means that organizations preparing SBOMs for CRA purposes, to meet security-related obligations, should not treat license data as optional or secondary. On the contrary, failing to track license obligations in the SBOM risks exposing the organization to legal liability, especially in complex supply chains or regulated industries.

SBOMs under the CRA are essential for:

- Ensuring compliance with security update obligations
- Supporting security vulnerability reporting (CRA Art. 14) and lifecycle risk management

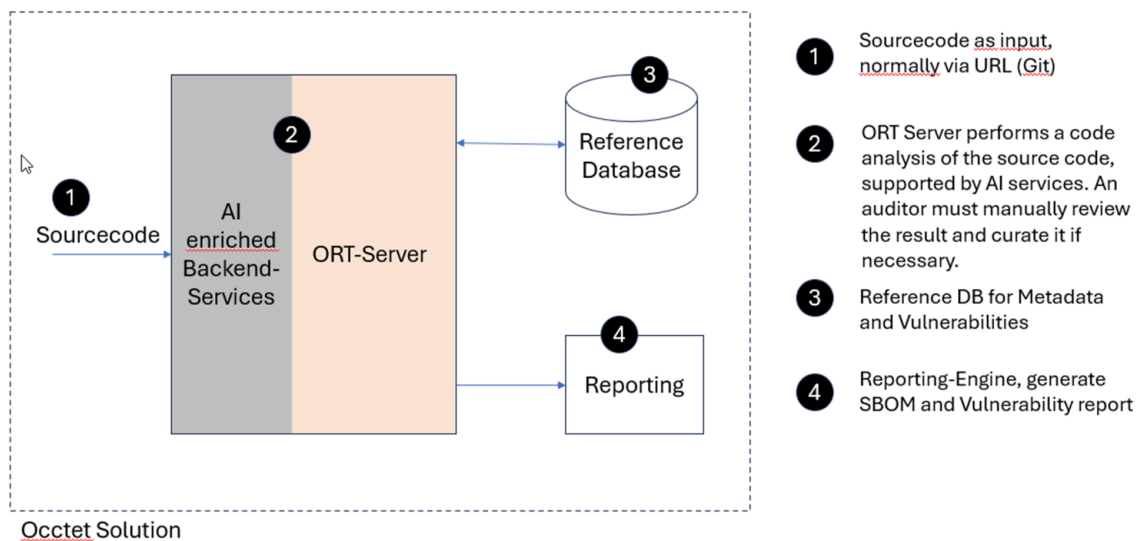
An SBOM fulfills several interrelated functions in the context of CRA compliance:



2 Introduction

2.1 Toolchain

The following graphic shows a high-level view of how the tools involved work together.



Each tool is presented in detail in the following sections, including its specific function, its integration points within the toolchain, and its technological foundations.

2.2 Testdata

2.2.1 Open Source Projects

The projects listed here were chosen since they host their source code on GitHub for easy comparison with [GitHub dependency insights](#) and [GitHub advanced security](#). The section 3.7.2 presents key numbers on the analysis of each of them.

- Eclipse Mosquitto (8,300+ GitHub Stars <https://github.com/eclipse/mosquitto> and Total 500M pulls on Docker https://hub.docker.com/_/eclipse-mosquitto),
- Jetty (3700 GitHub Stars <https://github.com/jetty/jetty.project>)
- Tomcat (7,200 GitHub stars <https://github.com/apache/tomcat>)
- Kafka (27,000+ GitHub stars <https://github.com/apache/kafka>)
- Hadoop (14,200 GitHub stars <https://github.com/apache/hadoop>)

In addition to the above list, section 3.7.1 presents the analysis results of 9-10 popular library projects from the following 10 ecosystems into use: C/C++, C#, Go, JVM (Java, Kotlin, Scala), JavaScript, PHP, Python, Ruby, Rust, Swift.



2.2.2 SME

- ReductSoftware UG, Christoph-Probst-Weg 4, 20251 Hamburg, Germany
 - ReductStore with the use cases
 - <https://github.com/reductstore/reduct-rs>
 - <https://github.com/reductstore/reductstore>
 - <https://github.com/reductstore/web-console>

While ReductSoftware is used here as an example, we can note that we are gathering testing feedback from several other testers with one or more use cases. We are developing the tooling further based on that, as part of our work in WP4. Currently we have five different testers with a total of nine use cases that have been set up, and we have an additional four testers with whom we are still in the process of setting up the testing activity.

The next section 3 goes through the CRA phases and how ORT Server supports that. ReductSoftware use cases are used as an example. The use cases of all testers that have completed the testing is very similar, so it is not useful to repeat such. Here are, however, some related observations from other testers:

- Of the currently tested nine use cases of the testers, we are able to support eight out of nine technologies among those use cases. These include software products, SaaS deliveries (with potential of applications relying on them) and IoT devices.
- One tester uses Yocto 5 (Scarthgap), and we introduced support for Yocto during 2026. The support for Yocto, as it is a widely used and developing linux distribution management system, including build steps, is being expanded, also as a part of feedback from this OCCTET tester, and the use cases will similarly grow.
- One tester/use case had a SaaS solution, but we are looking to complete testing with that use case anyhow, even though SaaS deployments are not directly CRA relevant, but there are certain interpretation issues and the CRA required controls (like vulnerability management) are useful also for SaaS deployments. The technologies in question seem straight forward to support.
- Some testers have open source projects. When doing testing with them we also recognize dependencies to private repositories for open source projects. As ORT Server also supports private repositories, this not an issue, but shows rather that sometimes use cases haven't realised themselves the dependencies that their project actually has.
- One tester/use case was investigated, but their build systems were not supported, since they used older versions of current systems and were not ready to upgrade to newer build systems. We decided not to build support for older versions of certain build systems within the OCCTET project. The not supported build systems in this case were Visual Studio Build Tools (VC2017) and CMake (v3.17.3).

occWe record here the legal names of current testers with whom the testing has been set up and use cases have been analyzed, at least initially. Further testing, or feedback may still be in the process:

- DH electronics GmbH
- Mahlo GmbH
- ReductSoftware UG
- A-SIT Plus GmbH
- Obeo S.A.S.



3 ORT Server (DOC)

3.1 Double Open's Role in OCCTET

Double Open Oy is a Finnish startup founded in the year 2023 that emerged out of a research and automation initiative by the Finnish law firm HH Partners which is engaged with the OpenChain project. Double Open strives for creating open solutions for highly automated software compliance checks and for process optimization. It does so via a unique combination of both legal and technical expertise in the open source domain, as the founders are top-tier technology attorneys and long-standing open source project maintainers.

Double Open's main product is the Double Open Compliance (DOC) solution. It is fully open source, building on and extending existing open source projects like the [OSS Review Toolkit \(ORT\)](#), the [ORT Server](#), and the [Double Open Server \(DOS\)](#). Simply speaking, one can think of DOC as a Double-Open-branded distribution of ORT Server with accompanying tools as well as optimal technical configuration and sound legal configuration. For the scope of this document, the terms "ORT Server" and "DOC" may be used interchangeably.

With the ORT ecosystem being central to Double Open's offerings, Double Open (co-)maintains these projects with an "upstream first" principle. Since the beginning of the OCCTET project, Double Open has publicly contributed more than 1700 changes and improvements to the wider ORT ecosystem. In particular, Double Open developed the whole Graphical User Interface (GUI) for the ORT Server in the form of a web frontend powered by the React framework.

The DOC solution serves the base platform to integrate with other OCCTET tools. Technically, this is archived via the different [plugin entry points](#) from the ORT ecosystem, including but not limited to vulnerability advisors, license scanners, and SBOM reporters.

3.2 Architectural Overview

The ORT Server is based on ORT, leveraging its libraries programmatically for component analysis, license scanning, vulnerability databases, compliance rules, and report generation. This allows users to manage and analyze dependencies and licenses with ease, offering detailed insights and compliance reporting.

A REST API is provided by ORT Server that allows for seamless integration with other tools and automation workflows. This API offers endpoints for performing tasks like managing repositories, secrets, or users, and getting the results of ORT runs, making it easy to incorporate ORT functionality into existing DevOps pipelines or CI/CD environments.

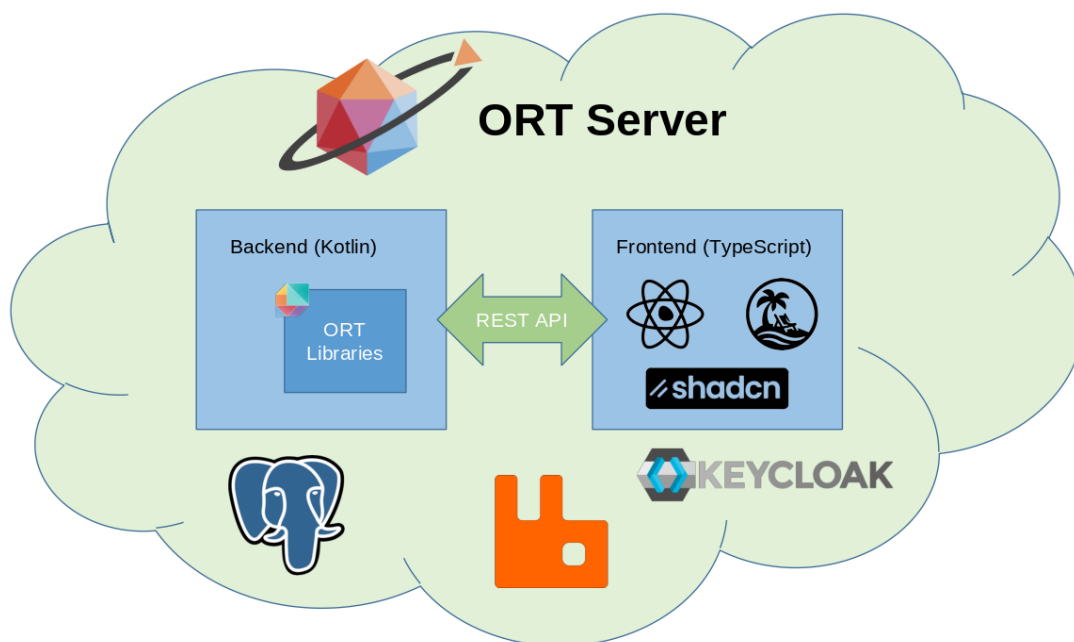


Following an API-first design, the ORT Server includes a React-based web UI that uses the REST API and is designed to streamline access to critical functions and data. This interface allows users to manage the compliance and security of their projects with ease, providing detailed reports of software components, licenses, and vulnerabilities.

Based on Keycloak as the identity and access management solution, ORT Server incorporates robust user access and role management capabilities. It supports user authentication, authorization, and multi-factor authentication, allowing organizations to define roles and permissions for different users. This ensures that different users can access only the relevant parts of the system.

To scale with a growing number of products throughout multiple organizations, ORT Server leverages Kubernetes as a container orchestration platform for efficient resource management and deployment. It allows organizations to scale their software composition analysis workflows horizontally by running the actual ORT components in separate containers. Kubernetes integration also provides enhanced automation, fault tolerance, and dynamic load balancing, ensuring high availability and reliability in production environments.

Put simply, the architecture can be depicted as follows:



The deployment is modularized into separate Docker images per worker (config, analyzer, advisor, reporter, etc.) to follow secure-by-design principles like minimizing the attack surface and using safe configuration out of the box. [Helm](#) charts are [provided](#) for convenient and easy setup of reproducible staging and production environments.



3.3 CRA Phases

On an abstract level, the activities from the CRA can be grouped into the following phases:

- **Initiation:** Product definition and applicability
- **Risk Assessment:** Intended / foreseeable use, support period, execution and documentation
- **Pre-launch:** Development practices, vulnerability handling, dependency management, SBOM generation
- **Post-launch:** Vulnerability monitoring, archiving

Out of these, the underlined requirements can theoretically be automated, and the following sections show how to do that with the DOC solution.

3.4 Vulnerability Management

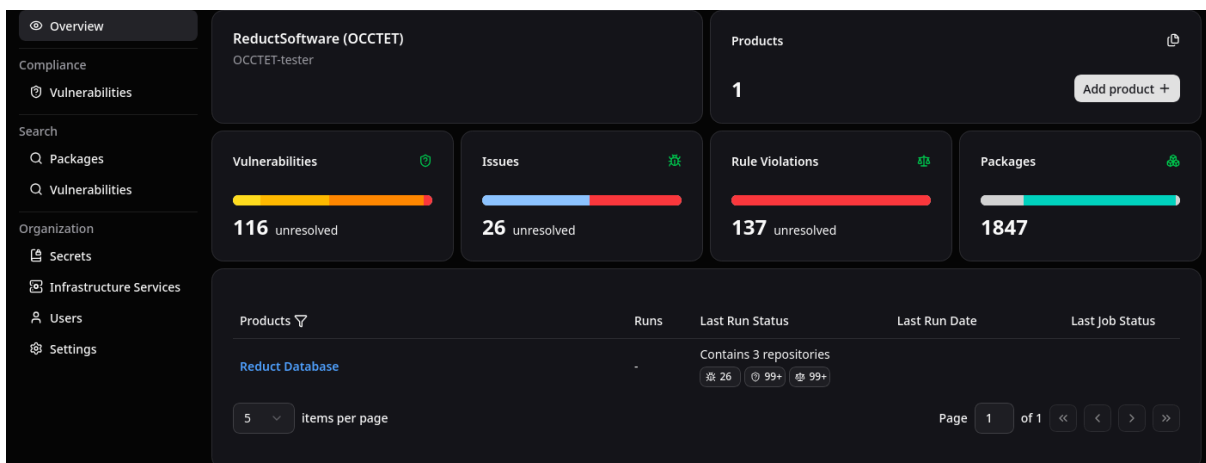
Note: For this section, the [ReductStore](#) OCCTET-tester will be used as an exemplary SME in the screenshots.

Getting an SME on-boarded in DOC starts with authentication, which is implemented via [Keycloak](#) Open Source Identity and Access Management (IAM) solution:



Accounts are either created in advance by a DOC administrator, or the user can authenticate via one of the configured Single Sign-On (SSO) integrations (as in the screenshot shown with *Google*, which includes Google Workspace account as commonly used in enterprises).

After logging in, the user lands at the SME organization's overview page. This hierarchical view allows for managing product groups to comply with the CRA's requirement of a **product definition**:



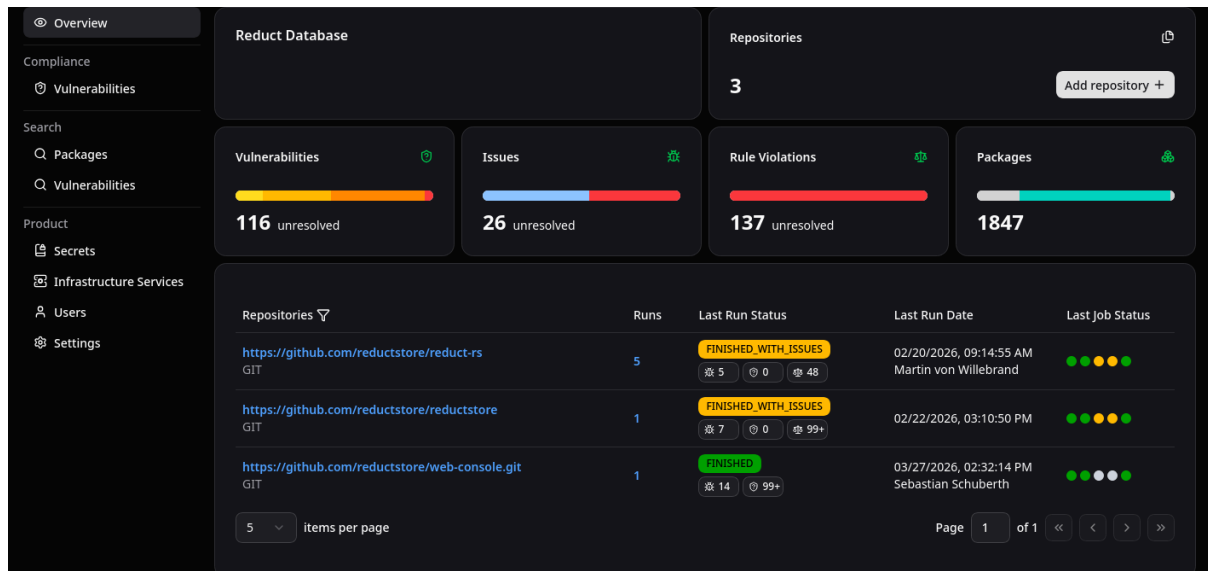
In this case, there is only a single product called *Reduct Database* inside the *ReductSoftware (OCCTET)* organization. To add new product definitions to the organization, the user clicks on the *Add product* button in the upper-right corner. A product is identified by a mandatory *Name* and has an optional *Description*:

Back on the organization's overview page, the central area shows a dashboard with *Vulnerabilities*, (technical) *Issues*, (policy) *Role Violations*, and statistics about the ecosystems *Packages* coming from all products throughout the organization. This view provides managers or security / legal staff with a compact overview of the compliance status in the organization.

By clicking on a name in the *Products* table, the user can go deeper in the hierarchy to manage the source code repositories a product is compromised of. A typical use-case is where a single product consists of both a backend and a frontend, which are implemented in



different programming languages and hosted in different repositories. At the example of the *Reduct Database* product, this is how it looks like on the product hierarchy level:



This product overview resembles the organization overview, but all dashboard numbers are scoped to the current product, which is useful e.g. for product owners. In a similar way to like products can be added to organization, *Repositories* can be added to products using the upper-right *Add repository* button:

Add Repository

URL

Description
(optional)

Type
Git
Git-Repo
Mercurial
Subversion

Currently, repositories are limited to Version Control System (VCS) repositories identified by a *URL* and *Type*. Again, an optional *Description* may be given.

Note: In the future, the source code of repositories can also be provided otherwise, like by the upload of a source code archive.



A user interested in **vulnerability handling** in the context of the CRA can then click on the *Vulnerabilities* card in the product overview dashboard. This takes the user to a table-view of vulnerabilities found in all repositories of the product:

Overview
Compliance
Vulnerabilities
Search
Packages
Vulnerabilities
Product
Secrets
Infrastructure Services
Users
Settings

Vulnerabilities (116 in total)

This is an overview of the vulnerabilities found within this product. It only takes into account the latest runs per repository that have successful advisor results. Please note that new vulnerabilities may get discovered over time. Therefore, your product's repositories should be scanned for vulnerabilities regularly, even if no code changes occurred.

	Package ID	Rating	External ID	Sort
pkg:npm/jsonpath@1.1.1 No summary available CRITICAL			CVE-2026-1615	1 repository
pkg:npm/form-data@3.0.1 form-data uses unsafe random function in form-data for choosing boundary CRITICAL			GHSA-fjwv-7rqg-78g4	1 repository
pkg:npm/jsonpath@1.1.1 JSONPath vulnerable to Prototype Pollution due to Insufficient L... CRITICAL			CVE-2025-61140	1 repository
pkg:npm/static-eval@2.0.2 Code Injection This CVE has been marked as a False Positive and ... CRITICAL			CVE-2021-23334	1 repository
pkg:npm/form-data@3.0.1 Use of Insufficiently Random Values vulnerability in form-data a... CRITICAL			CVE-2025-7783	1 repository
pkg:npm/node-forge@1.3.1 node-forge has ASN.1 Unbounded Recursion HIGH			GHSA-554w-wp2-vwz7	1 repository
pkg:npm/body-parser@1.20.2 body-parser vulnerable to denial of service when url encoding is enabled HIGH			GHSA-qwcr-v2fm-qrc7	1 repository

In this example case, all vulnerabilities stem from Node Package Manager (NPM) packages in a single repository. However, in general a vulnerable package could be part of multiple repositories. In order to find out which repositories contain a vulnerable package, currently a manual step is involved which requires the user to copy the package identifier in [Package URL](#) (PURL) format starting with "pkg:" to the clipboard via the -icon. Then the user needs to navigate to the *Packages* search in the left-hand menu and paste the PURL from the clipboard to the *Search Packages* field (which is interpreted as a regular expression). The search result then looks like

Search Package
Search for ORT runs in repositories of this product that contain matching packages.

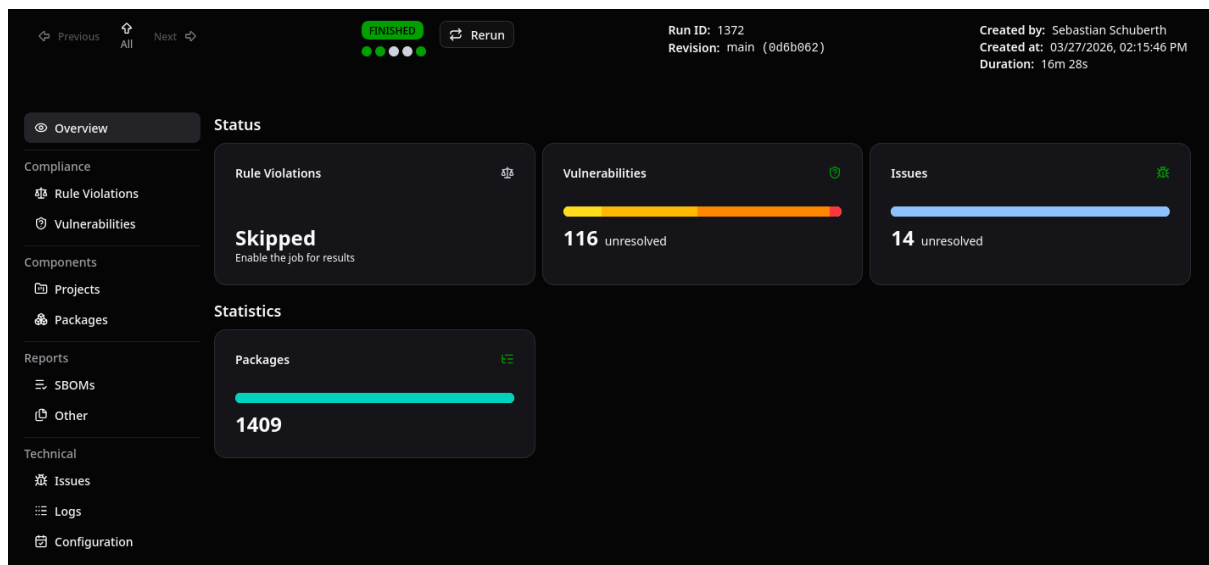
pkg:npm/jsonpath@1.1.1

Created At	Repository	Revision	Run Index	Matching Package
03/27/2026, 02:15:46 PM	https://github.com/reductstore/web-console.git	main	1	pkg:npm/jsonpath@1.1.1

10 items per page
Page 1 of 1



Clicking on the *Run Index* link of a result row in the table takes the user straight of the compliance run on the respective repository where the package was discovered via Software Composition Analysis (SCA) when running ORT's Analyzer tool. This is how the overview page for a compliance run on the repository level looks like:



Clicking once more on the *Vulnerabilities* card opens up the run-centric view of vulnerability details:

Vulnerabilities (116 in total, 116 matching filters)

This view shows the vulnerabilities found in any of the packages used as dependencies of a project. As vulnerabilities may be only discovered over time, new vulnerabilities may arise even without changes to the any of the projects or their dependencies. Therefore, it is important to check for vulnerabilities on a regular basis.

Package ID	Status	Rating	External ID	Sort
pkg:npm/static-eval@2.0.2	Unresolved	CRITICAL	CVE-2021-23334	
Code Injection This CVE has been marked as a False Positive and ...			VulnerableCode	
pkg:npm/jsonpath@1.1.1	Unresolved	CRITICAL	CVE-2025-61140	
JSONPath vulnerable to Prototype Pollution due to Insufficient L...			VulnerableCode	
pkg:npm/form-data@3.0.1	Unresolved	CRITICAL	CVE-2025-7763	
Use of Insufficiently Random Values vulnerability in form-data a...			VulnerableCode	
pkg:npm/jsonpath@1.1.1	Unresolved	CRITICAL	CVE-2026-1615	
No summary available			VulnerableCode	
pkg:npm/form-data@3.0.1	Unresolved	CRITICAL	GHSA-fpwx-7qgq-78g4	
form-data uses unsafe random function in form-data for choosing boundary			OSV	

Each card in the table view contains a summary of the vulnerability and the name of the advisor that provided the vulnerability data. The first four vulnerabilities came in via ORT's advisor plugin for **AboutCode's (ABCD)** VulnerableCode platform, whereas the last vulnerability in the screenshots came in via the Google OSV advisor plugin of ORT.



In order to review and handle a specific vulnerability, the user can click on the -icon to expand the details panel for a specific vulnerability finding:

pkg:npm/static-eval@2.0.2

Code Injection This CVE has been marked as a False Positive and ...

Unresolved CRITICAL

CVE-2021-23334

VulnerableCode

Create a resolution

Reason

CANT_FIX_VULNERABILITY

Comment

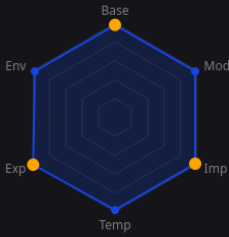
Add a comment...

Create resolution

Details

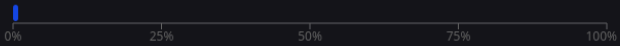
CVSS 3.1 Severity Radar (details)

Severity scores from CVSS assessing impact and exploitability of the vulnerability.



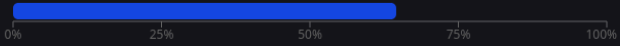
EPSS Score (details)

Probability of observing exploitation activity in the wild in the next 30 days.



EPSS Percentile (details)

Relative ranking of exploit probability compared to all scored vulnerabilities.



Description

Code Injection This CVE has been marked as a False Positive and has been removed.

Links to vulnerability references

Severity	Scoring system	Score	Vector	Link
CRITICAL	cvssv3.1	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	https://github.com/browserify/static-eval/blob/master/index.js%23L180
CRITICAL	cvssv3.1	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1071860

This view allows investigating the details of the vulnerability and to follow any of the reference links for yet more background information.

If the manual investigation by a security expert user comes to the conclusion that the vulnerability finding should be resolved, this can be done from the panel to *Create a resolution*:



Create a resolution

Reason

NOT_A_VULNERABILITY ▾

- CANT_FIX_VULNERABILITY
- INEFFECTIVE_VULNERABILITY
- INVALID_MATCH_VULNERABILITY
- MITIGATED_VULNERABILITY
- NOT_A_VULNERABILITY ✓
- WILL_NOT_FIX_VULNERABILITY
- WORKAROUND_FOR_VULNERABILITY

Det

In this case, having a closer look at the summary information of the vulnerability reveals that it is a false-positive: “[...] This CVE has been marked as a False Positive and has been removed.”

So a viable option is to resolve this finding as *NOT_A_VULNERABILITY*. After clicking on *Create resolution*, the resolution is saved and will be applied on the next compliance run on the repository:

NOT_A_VULNERABILITY Created: pending rerun SERVER

This CVE has been marked as a False Positive and has been removed.

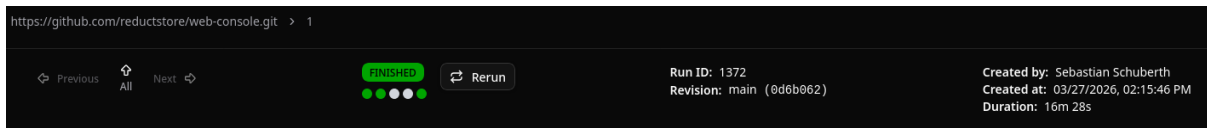
ID Matcher: CVE-2021-23334

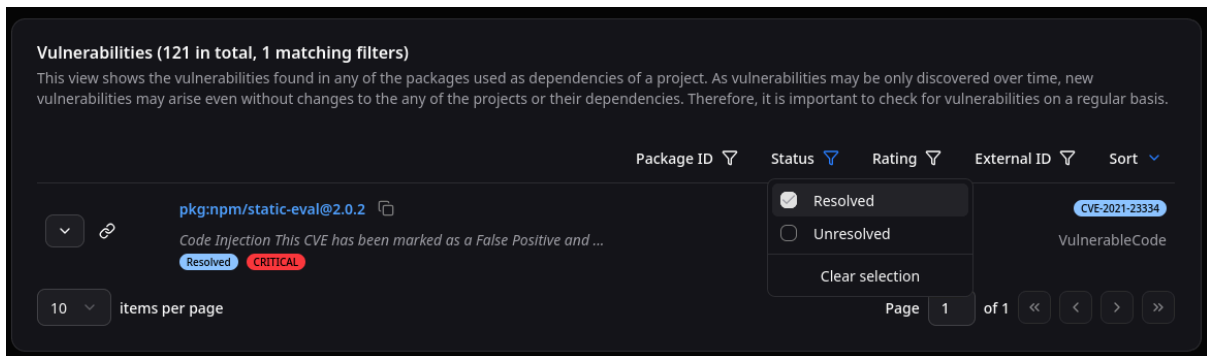
Resolutions can be edited and deleted as needed via the respective icons on the right-hand side. Above these icons, the *SERVER* badge indicates that the resolution is managed on the server-side, as opposed to a resolution created via [configuration-as-code](#) by committing a *.ort.yml* file repository.

Note: The concrete names of the vulnerability resolution reasons are currently being reworked to more closely resemble CRA use-cases.

The user can now trigger *Rerun* from the top-level header controls to apply the pending changes:



The new run then shows the vulnerability as resolved:



Note: The first run had 116 vulnerability findings in total, while the second run has 121 in total (out of which 1 is resolved). The difference of 5 findings is due to the fact that during the time between runs 1 and 2 those 5 new vulnerabilities have been discovered in the transitive dependencies of the projects in the repository although no code changes have been made to the project itself. This is a prime example for why **vulnerability monitoring** is crucial.

The monitoring of vulnerabilities of released or in-development products can currently be implemented with the help of the accompanying [GitHub action](#) which leverages the [ORT Server CLI \(OSC\)](#) to schedule runs via the [REST API](#) of ORT Server. By creating a [GitHub workflow with a schedule](#) that uses the ORT Server action, runs are regularly triggered on the server even without code changes to the product.

3.5 Dependency Management

There is a connection between vulnerability management and dependency management in the sense that dependencies of a project have to be discovered before they can be checked for known vulnerabilities, and because addressing a vulnerability by updating a dependency to a fixed version is easier for direct dependencies than for transitive dependencies (dependencies of dependencies) of a project.

This is why ORT Server provides best-in-class Software Composition Analysis (SCA) for software projects via the ORT Analyzer tools. In contrast to many other (including commercial) solutions, the ORT Analyzer does not require to modify or prepare the project under analysis (e.g. by applying build system plugins), and it analyzes project dependencies dynamically, taking into account any version conflict resolution applied by the build system, which results in a deviation of the statically declared dependencies in the project manifests.



In order to achieve this depth of knowledge, the ORT Analyzer relies and (implicitly) checks for good **development practices** when managing dependencies in the build system. Technical *Issues* are raised if a project is set up in a way that prevents the SCA to function properly, or *Deprecation* hints are filed if outdated dependencies are found even if they are not known to be vulnerable:

Issues (14 in total, 14 matching filters)

This view shows any technical issues that were discovered by the respective source. As technical issues might have an impact on the completeness of metadata, it is highly recommended to resolve any technical issues before acting on any compliance related findings.

Package ID ▾ Status ▾ Severity ▾ Category ▾ Sort ▾

[NPM::web-console:1.14.0-beta.1](#)

Created at 03/28/2026, 07:33:35 AM by analyzer

Unresolved HINT Deprecation

Resolutions ▾

Details ▴

deprecated @babel/plugin-proposal-class-properties@7.18.6: This proposal has been merged to the ECMAScript standard and thus this plugin is no longer maintained. Please use @babel/plugin-transform-class-properties instead.

ORT Server provides means to inspect a vulnerability for its dependency relationship to the project. In order to do so, a user navigates to the Vulnerabilities view and clicks on the blue package ID within a card in the table:

Vulnerabilities (121 in total, 120 matching filters)

This view shows the vulnerabilities found in any of the packages used as dependencies of a project. As vulnerabilities may be only discovered over time, new vulnerabilities may arise even without changes to the any of the projects or their dependencies. Therefore, it is important to check for vulnerabilities on a regular basis.

Inspect the package details in packages table

Package ID ▾ Status ▾ Rating ▾ External ID ▾ Sort ▾

[pkg:npm/jsonpath@1.1.1](#)

JSONPath vulnerable to Prototype Pollution due to Insufficient I...

Unresolved CRITICAL CVE-2025-61140 VulnerableCode

This tackles a user straight to the expanded details of that specific package, which contains information about the *Shortest Dependency Paths* at the bottom of the details panel:



Packages (1409 in total, 1 matching filters)
This view shows the flat set of de-duplicated packages discovered for all projects.

Package ID Declared License Sort

pkg:npm/jsonpath@1.1.1 <https://github.com/dchester/jsonpath#readme>

Declared License: MIT

Authors: david@fmail.co.uk

Description
Query JavaScript objects with JSONPath expressions. Robust / safe JSONPath engine for Node.js.

CPE: N/A

Source Code Origins: N/A

Git Repository
URL: <https://github.com/dchester/jsonpath.git>
Revision: c1dd8ec74034fb037523abb5fdbec51ac317b4b
Path: N/A

Binary Artifact: N/A

Source Artifact
URL: <https://registry.npmjs.org/jsonpath/-/jsonpath-1.1.1.tgz>
Hash Value: 0ca1ed8fb65bb3309248cc9d5466d12d5b0b9901
Hash Algorithm: SHA-1

Shortest Dependency Paths
NPM::web-console:1.14.0-beta.1 (scope 'devDependencies') → pkg:npm/react-scripts@5.0.1 → pkg:npm/bfj@7.1.0 → pkg:npm/jsonpath@1.1.1

Labels: N/A

10 items per page

Page 1 of 1

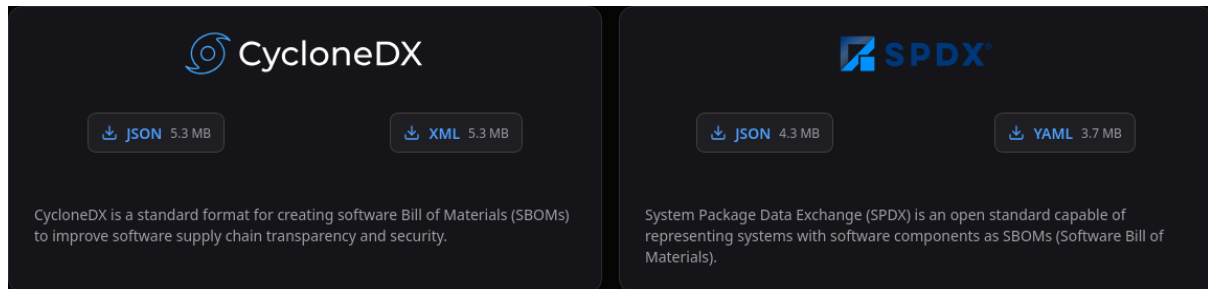
This shows that the **pkg:npm/jsonpath@1.1.1** package is a transitive dependency within the *devDependencies* scope of the **NPM::web-console:1.14.0-beta.1** project, which has been introduced via the direct dependency on **pkg:npm/react-scripts@5.0.1** and its **pkg:npm/bfj@7.1.0** dependency. So in this case upgrading the **pkg:npm/jsonpath@1.1.1** package directly in the **NPM::web-console:1.14.0-beta.1** project is not possible, and the user needs to wait for or work with the projects along the *Shortest Dependency Paths* to upgrade to a non-vulnerable version of the **pkg:npm/jsonpath@1.1.1** package.

Note: A future version of ORT Server will make it easier for the user to understand whether a newer version of a package is available that fixes the vulnerability, and how to upgrade to it depending on whether the dependency is direct or transitive to the project.

3.6 SBOM Generation

Based on the metadata gathered during the analyzer and advisor phases, ORT Server can create various reports, including Software Bill-of-Materials (SBOMs), compulsory statements, disclosure documents, vulnerability reports, source code archives, and [many more](#). These can be accessed from the *Reports* menu of a run.

For the two most widely used SBOM formats, CycloneDX and SPDX, ORT Server offer a dedicated page to download these reports in various formats from:



Note: While ORT currently offers more detailed options to configure these SBOMs, like the exact version to the output file format specification to use, these options are not yet exposed as part of the ORT Server UI.

While ORT offers a dedicated report template for vulnerabilities, by now the [OpenVEX](#) standard gains adoption as a format to exchange data about the exploitability of a vulnerability in a given product context. As it makes sense to track the static data about dependencies in an SBOM separately from the dynamic data about known vulnerabilities in these dependencies, ORT will feature a separate VEX reporter going forward.

3.7 ORT Dependency and Vulnerability Analysis of Popular Open Source Projects

Besides testing with software products from [SMEs](#), the toolchain around ORT Server has also been run on 96 popular open source projects and several renowned open source projects for testing.

3.7.1 Popular Open Source Projects

3.7.1.1 Introduction

As part of the OCCTET WP3 efforts for D3.3, and in collaboration with WP4 task 4.4, 96 widely-used open source projects were selected for automated analysis using the ORT (OSS Review Toolkit) platform hosted on the OCCTET ORT Server (ort-server.occtet.eu). Projects are organised into ten language ecosystems: C/C++, C#, Swift, Rust, Ruby, Python, Go, PHP, JavaScript, and JVM, with approximately ten repositories per ecosystem selected on the basis of download counts and community adoption metrics. ORT resolves the full transitive dependency graph for each project and runs advisor jobs against the OSV and VulnerableCode advisory databases to surface known vulnerabilities. This report presents, for each ecosystem and repository: the analysis pipeline status, the total number of third-party packages identified, and the vulnerability findings broken down by severity. The five repositories with the highest vulnerability counts are examined in further detail, with per-package advisory listings and upgrade recommendations available directly from ORT Server.



The data extraction in this section 3.7.1 has benefited from the ORT Server API's and AI agents have been used to compile the data into tables. Also, UI screenshot examples have been added to show the “human” UI view.

3.7.1.2 Overall Summary

Ecosystem	Started	Clean	Analysis Issues	Failed	Vulns	Deps
C/C++ Projects	10	3	7	0	488	1395
C# Projects	10	6	4	0	45	2466
Swift Projects	10	9	1	0	295	972
Rust Projects	10	9	1	0	83	997
Ruby Projects	10	5	5	0	111	760
Python Projects	10	9	1	0	27	427
Go Projects	9	8	1	0	0	8
PHP Projects	10	8	2	0	25	431
JavaScript Projects	10	10	0	0	66	628
JVM Projects	7	7	0	0	55	243
Total	96	74	22	0	1112	6471

Status definitions:

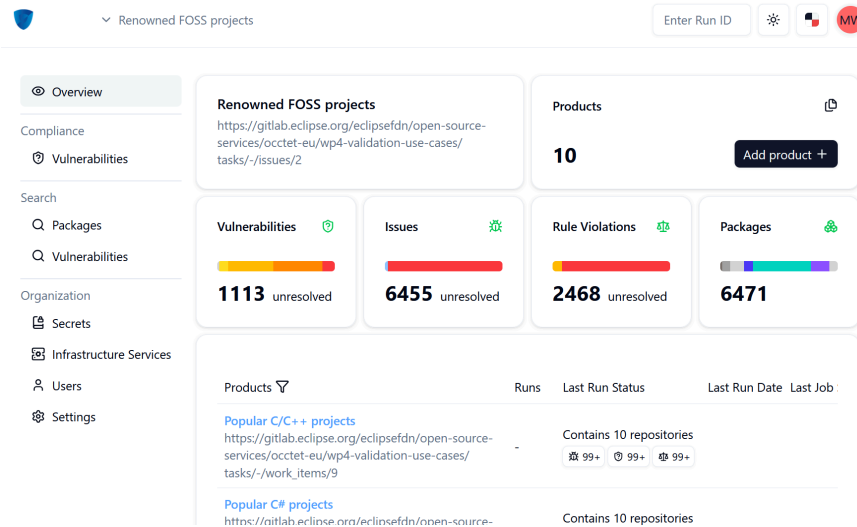
Clean: the analyzer completed without issues; issues in later pipeline stages (scanner, evaluator, reporter) do not affect this classification.

Analysis Issues: the analyzer job completed but reported one or more issues, typically relating to sub-projects or files that could not be resolved in ORT's analysis environment; these are often opportunities to improve practices in the target project, as ORT works best with best practice development methods.

Failed: no analysis run fails.

Vulns: total number of vulnerabilities–package pair findings reported by the ORT advisor (see the Vulnerability Findings section for an explanation of this counting method).

Deps: total number of third-party packages identified in the transitive dependency graph for the most recent run.



UI view:

C/C++ Projects

Repository	Status	Deps	Vulns
boostorg/boost	Analysis Issues	426	163
curl/curl	Analysis Issues	46	0
ffmpeg/ffmpeg	Clean	0	0
gabime/spdlog	Clean	0	0
madler/zlib	Analysis Issues	15	0
opencv/opencv	Analysis Issues	282	82
open-source-parsers/jsoncpp	Clean	21	0
openssl/openssl	Analysis Issues	332	138
protocolbuffers/protobuf	Analysis Issues	200	5
qt/qtbase	Analysis Issues	195	100

C# Projects

Repository	Status	Deps	Vulns
App-vNext/Polly	Clean	114	0
AutoMapper/AutoMapper	Clean	28	0
AvaloniaUI/Avalonia	Analysis Issues	932	15
DapperLib/Dapper	Clean	162	0
dotnet/runtime	Analysis Issues	0	0
FluentValidation/FluentValidation	Analysis Issues	120	12
JamesNK/Newtonsoft.Json	Clean	58	0
NLog/NLog	Analysis Issues	151	19
restsharp/RestSharp	Clean	1490	14
serilog/serilog	Clean	64	0



Swift Projects

Repository	Status	Deps	Vulns
Alamofire/Alamofire	Clean	54	1
Kitura/Kitura	Clean	25	0
Moya/Moya	Clean	55	33
mxcl/PromiseKit	Analysis Issues	745	257
onevcatt/Kingfisher	Clean	122	2
PerfectlySoft/Perfect	Clean	1	0
ReactiveX/RxSwift	Clean	26	8
SnapKit/SnapKit	Clean	0	0
SwiftyJSON/SwiftyJSON	Clean	0	0
vapor/vapor	Clean	28	0

Rust Projects

Repository	Status	Deps	Vulns
BurntSushi/memchr	Analysis Issues	76	1
cuviper/autocfg	Clean	0	0
dtolnay/proc-macro2	Clean	58	0
dtolnay/quote	Clean	29	0
dtolnay/unicode-ident	Clean	173	1
matklad/once_cell	Clean	8	0
microsoft/windows-rs	Clean	800	82
rust-lang/cfg-if	Clean	0	0
rust-lang/libc	Clean	33	0
rust-lang/log	Clean	29	0

Ruby Projects

Repository	Status	Deps	Vulns
guard/guard	Clean	51	0
jnunemaker/httparty	Clean	57	2
lostisland/faraday	Clean	261	11
rack/rack	Analysis Issues	24	0
rails/rails	Analysis Issues	499	94
rails/thor	Clean	56	1
rest-client/rest-client	Clean	41	7
ruby/json	Analysis Issues	0	0
sparklemotion/nokogiri	Analysis Issues	0	0
sparklemotion/sqlite3-ruby	Analysis Issues	0	0



Python Projects

Repository	Status	Deps	Vulns
benjaminp/six	Clean	0	0
certifi/python-certifi	Clean	0	0
dateutil/dateutil	Clean	49	17
jawah/charset_normalizer	Clean	46	2
kjd/idna	Clean	0	0
numpy/numpy	Analysis Issues	366	8
psf/requests	Clean	50	0
pypa/packaging	Clean	2	0
python/typing_extensions	Clean	0	0
urllib3/urllib3	Clean	0	0

Go Projects

Repository	Status	Deps	Vulns
davecgh/go-spew	Clean	0	0
go-yaml/yaml	Analysis Issues	0	0
modern-go/concurrent	Clean	0	0
modern-go/reflect2	Clean	0	0
pkg/errors	Clean	0	0
pmezard/go-difflib	Clean	0	0
spf13/pflag	Clean	0	0
stretchr/testify	Clean	5	0
golang.org/x/text	Clean	3	0

PHP Projects

Repository	Status	Deps	Vulns
doctrine/dbal	Clean	87	0
doctrine/orm	Clean	67	0
guzzle/guzzle	Analysis Issues	89	0
laravel/framework	Clean	219	3
php-fig/log	Clean	0	0
Seldaek/monolog	Clean	76	0
symfony/console	Clean	28	0
symfony/dependency-injection	Analysis Issues	15	0
symfony/yaml	Clean	10	0
twigphp/Twig	Clean	84	24

JavaScript Projects



Repository	Status	Deps	Vulns
feross/safe-buffer	Clean	273	2
inspect-js/hasOwn	Clean	1	0
isaacs/inherits	Clean	0	0
isaacs/node-graceful-fs	Clean	182	28
ljharb/has-symbols	Clean	0	0
lydell/js-tokens	Clean	110	32
microsoft/tslib	Clean	136	4
npm/wrappy	Clean	0	0
Raynos/function-bind	Clean	0	0
TooTallNate/util-deprecate	Clean	0	0

JVM Projects

Repository	Status	Deps	Vulns
external/jsr-305	Clean	0	0
apache/commons-logging	Clean	65	16
apache/commons-collections	Clean	24	2
eclipse-ee4j/injection-api	Clean	0	0
google/guava	Clean	113	35
JetBrains/java-annotations	Clean	45	0
qos-ch/slf4j	Clean	11	2

3.7.1.3 Vulnerability Findings

Vulnerability data was collected by the ORT advisor step using the OSV and VulnerableCode advisory databases. The table below aggregates findings by ecosystem across all repositories with a completed ORT run. Counting methodology: each row in the ORT vulnerability output represents one advisory–package pair — that is, one known advisory (CVE, GHSA or similar) matched against one specific package version in the dependency graph. If the same advisory affects five packages, it is counted five times. Totals therefore reflect the volume of findings to triage, not the number of distinct advisories or distinct vulnerable packages. The per-repository deep dives in the following subsections present findings grouped by package, with all advisory IDs for each package collected into a single row.

Ecosystem	Critical	High	Medium	Low	None	Total
C/C++ Projects	29	204	209	31	15	488
C# Projects	3	19	21	2		45
Swift Projects	62	133	72	25	3	295
Rust Projects	2	37	33	10	1	83
Ruby Projects	7	44	55	5		111
Python Projects	2	14	9		2	27
Go Projects						



PHP Projects	2	4	7	12		25
JavaScript Projects	6	33	26	1		66
JVM Projects	7	20	27	1		55
Total	120	508	459	87	21	1195

3.7.1.4 Top 5 Repositories by Vulnerability Count

The five repositories with the highest total vulnerability counts are examined in greater detail below. This demonstrates the capabilities of the platform, identifying vulnerabilities in dependencies and providing information about the upgrade paths to those vulnerable dependencies.

For each repository the following information is provided: the Git URL, the analysed version tag with commit date, the total package count with a breakdown by package manager, and the vulnerability mix across severity levels. This is followed by a table of five packages with critical or high severity vulnerability advisories. Each table row represents one package version; the Advisories column lists all advisory IDs (CVE, GHSA) that affect that package, and the Upgrade / Fix column gives the minimum fixed version as reported by ORT Server, where available. Medium and Low severity findings are included in the counts but not individually listed.

mxcl/PromiseKit

Repository: <https://github.com/mxcl/PromiseKit.git>

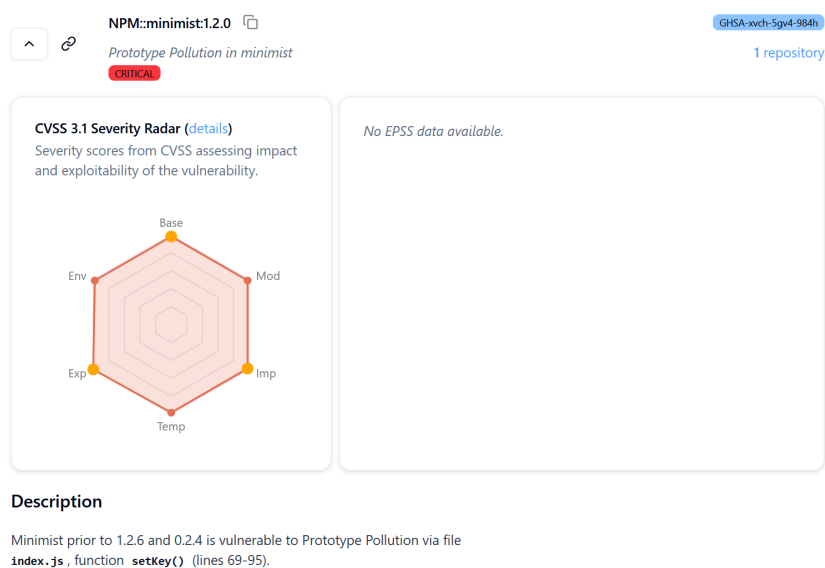
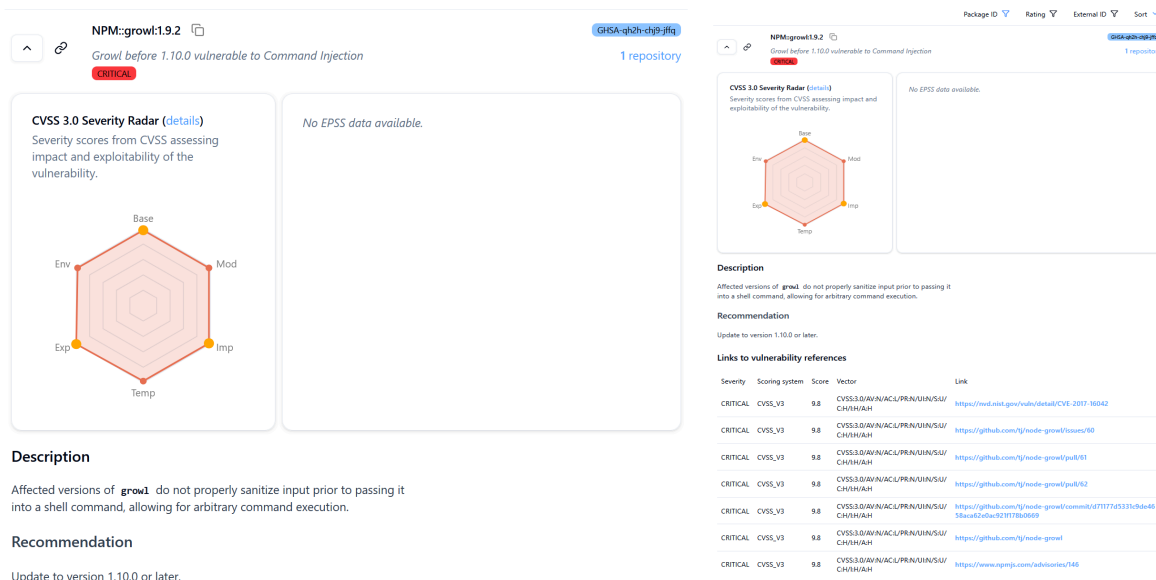
Version analysed: 8.2.0 (commit 2025-01-16) | ORT run: 2026-05-27

Dependencies: 745 packages (Carthage: 10, NPM: 733, Swift: 2)

Vulnerabilities: 253 total — Critical: 60, High: 119, Medium: 52, Low: 22

Package	Sev.	Score	Advisories	Upgrade / Fix
growl@1.9.2	Critical	9.8	GHSA-qh2h-chj9-jffq, GMS-2016-47, CVE-2017-16042	≥ 1.10.0
minimist@0.0.8	Critical	9.8	GHSA-xvch-5gv4-984h, CVE-2021-44906, CVE-2020-7598, GHSA-7fhm-mqm4-2wp7, GHSA-vh95-rmgr-6w4m	≥ 1.2.6
minimist@0.1.0	Critical	9.8	GHSA-xvch-5gv4-984h, CVE-2021-44906, CVE-2020-7598, GHSA-7fhm-mqm4-2wp7, GHSA-vh95-rmgr-6w4m	≥ 1.2.6
minimist@1.2.0	Critical	9.8	GHSA-xvch-5gv4-984h, CVE-2021-44906, CVE-2020-7598, GHSA-7fhm-mqm4-2wp7, GHSA-vh95-rmgr-6w4m	≥ 1.2.6
tough-cookie@2.3.4	Critical	9.8	CVE-2023-26136, GHSA-72xf-g2v4-qvf3	≥ 4.1.3

Example 1 UI view (zoomed-in, and zoomed-out), showcasing the advisory presentation, including affected package, advisory id, severity, affected versions, upgrade path and links to references:



Example 2 UI view:

boostorg/boost

Repository: <https://github.com/boostorg/boost.git>

Version analysed: master (commit 2026-05-23) | ORT run: 2026-05-27

Dependencies: 426 packages (Crate: 109, NPM: 286, PyPI: 31)

Vulnerabilities: 157 total — Critical: 18, High: 61, Medium: 67, Low: 11



Package	Sev.	Score	Advisories	Upgrade / Fix
axios@1.12.2	Critical	10.0	CVE-2025-62718, CVE-2026-40175, GHSA-43fc-jf86-j433, GHSA-6chq-wfr3-2hj9, GHSA-pf86-5x62-jrwf, GHSA-pmwg-cvhr-8vh7, GHSA-q8qp-cvcw-x6jj, CVE-2026-25639, GHSA-3p68-rc4w-qgx5, GHSA-3w6x-2g7m-8v23, GHSA-445q-vr5w-6q77, GHSA-5c9x-8gcm-mpgx, GHSA-62hf-57xw-28j9, GHSA-m7pr-hjqh-92cm, GHSA-vf2m-468p-8v99, GHSA-w9j2-pvgh-6h63, GHSA-xx6v-rp6x-q39c, GHSA-fvcv-3m26-pcqx, GHSA-xhjh-pmcv-23jw	≥ 1.13.5
axios@1.13.5	Critical	10.0	CVE-2025-62718, CVE-2026-40175, GHSA-6chq-wfr3-2hj9, GHSA-pf86-5x62-jrwf, GHSA-pmwg-cvhr-8vh7, GHSA-q8qp-cvcw-x6jj, GHSA-3p68-rc4w-qgx5, GHSA-3w6x-2g7m-8v23, GHSA-445q-vr5w-6q77, GHSA-5c9x-8gcm-mpgx, GHSA-62hf-57xw-28j9, GHSA-m7pr-hjqh-92cm, GHSA-vf2m-468p-8v99, GHSA-w9j2-pvgh-6h63, GHSA-xx6v-rp6x-q39c, GHSA-fvcv-3m26-pcqx, GHSA-xhjh-pmcv-23jw	≥ 1.15.1
axios@1.13.2	Critical	10.0	CVE-2025-62718, CVE-2026-40175, GHSA-43fc-jf86-j433, GHSA-6chq-wfr3-2hj9, GHSA-pf86-5x62-jrwf, GHSA-pmwg-cvhr-8vh7, GHSA-q8qp-cvcw-x6jj, CVE-2026-25639, GHSA-3p68-rc4w-qgx5, GHSA-3w6x-2g7m-8v23, GHSA-445q-vr5w-6q77, GHSA-5c9x-8gcm-mpgx, GHSA-62hf-57xw-28j9, GHSA-m7pr-hjqh-92cm, GHSA-vf2m-468p-8v99, GHSA-w9j2-pvgh-6h63, GHSA-xx6v-rp6x-q39c, GHSA-fvcv-3m26-pcqx, GHSA-xhjh-pmcv-23jw	≥ 1.13.5
handlebars@4.7.8	Critical	9.8	GHSA-2w6w-674q-4c4q, CVE-2026-33937, GHSA-3mfm-83xf-c92r, GHSA-9cx6-37pm-9jff, GHSA-xhpn-hc6g-r9c6, GHSA-xjpj-3mr7-gcpf, CVE-2026-33938, CVE-2026-33940, CVE-2026-33941, CVE-2026-33939, GHSA-2qvq-rjwj-gvw9, GHSA-7rx3-28cr-v5wh, CVE-2026-33916, GHSA-442j-39wm-28r2	≥ 4.7.9
convict@6.2.4	Critical	9.4	GHSA-44fc-8fm5-q62h, GHSA-hf2r-9gf9-rwch, CVE-2026-33864, CVE-2026-33863	≥ 6.2.5

openssl/openssl

Repository: <https://github.com/openssl/openssl.git>



Version analysed: master (commit 2026-05-27) | ORT run: 2026-05-27

Dependencies: 332 packages (Crate: 156, Go: 2, PyPI: 174)

Vulnerabilities: 129 total — Critical: 0, High: 49, Medium: 69, Low: 11

Package	Sev.	Score	Advisories	Upgrade / Fix
openssl@0.10.71	High	9.3	GHSA-8c75-8mhr-p7r9, GHSA-ghm9-cr32-g9qj, GHSA-hppc-g8h3-xhp3, GHSA-pqf5-4pqq-29f5, GHSA-xp3w-r5p5-63rr, GHSA-4fcv-w3qc-ppgg, GHSA-xv59-967r-8726, GHSA-phqj-4mhp-q6mq, GHSA-xmgf-hq76-4vx2, RUSTSEC-2025-0022	≥ 0.10.78
urllib3@2.3.0	High	8.9	GHSA-38jv-5279-wg99, GHSA-2xpw-w6gg-jr37, GHSA-gm62-xv2j-4w53, GHSA-qccp-gfcp-xxvc, CVE-2025-66418, CVE-2026-21441, CVE-2026-44431, CVE-2025-66471, GHSA-48p4-8xcf-vxj5, GHSA-pq67-6m6q-mj2v, PYSEC-2026-141, CVE-2025-50181, CVE-2025-50182	≥ 2.6.3
setuptools@78.1.0	High	8.8	GHSA-5rjg-fvgr-3xxf, PYSEC-2025-49, CVE-2025-47273	≥ 78.1.1
typed-ast@1.2.0	High	8.7	CVE-2019-19275, CVE-2019-19274, PYSEC-2019-130, PYSEC-2019-131	≥ 1.3.2
cryptography@44.0.3	High	8.2	GHSA-r6ph-v2qm-q3c2, CVE-2026-26007, PYSEC-2026-35, CVE-2026-34073, GHSA-m959-cc7f-wv43	≥ 46.0.5

qt/qtbase

Repository: <https://github.com/qt/qtbase.git>

Version analysed: dev (commit 2026-05-27) | ORT run: 2026-05-27

Dependencies: 195 packages (Maven: 166, NPM: 26, PyPI: 3)

Vulnerabilities: 100 total — Critical: 4, High: 55, Medium: 37, Low: 4

Package	Sev.	Score	Advisories	Upgrade / Fix
bcprov-jdk18on@1.79	Critical	10.0	CVE-2026-5598, GHSA-p93r-85wp-75v3, GHSA-c3fc-8qff-9hwx, CVE-2026-0636	≥ 1.84



lodash@4.17.10	Critical	9.8	GHSA-jf85-cpcp-j695, CVE-2019-10744, GHSA-r5fr-rjxr-66jc, GHSA-35jh-r3h4-6jhm, GHSA-4xc9-xhrj-v574, GHSA-p6mc-m468-83gw, CVE-2018-16487, CVE-2025-13465, CVE-2021-23337, CVE-2020-28500, CVE-2026-4800, CVE-2020-8203, GHSA-f23m-r3pf-42rh, GHSA-xxjr-mmjv-4gpg, GHSA-29mw-wpgm-hmr9, GHSA-x5rq-j2xg-h7qm, CVE-2026-2950, CVE-2019-1010266	≥ 4.17.12
netty-handler@4.1.93 .Final	Critical	9.1	CVE-2023-34462, GHSA-4g8c-wm8x-jfhw, CVE-2025-24970, CVE-2023-4586, GHSA-6mj-q-h674-j845	≥ 4.1.118.Final
netty-codec-http2@4.1.110.Final	High	8.7	GHSA-w9fj-cfpg-grvv, GHSA-prj3-ccx8-p6x4, GHSA-f6hv-jmp6-3vvw, CVE-2026-33871	≥ 4.1.132.Final
netty-codec-http2@4.1.93.Final	High	8.7	GHSA-w9fj-cfpg-grvv, GHSA-prj3-ccx8-p6x4, GHSA-f6hv-jmp6-3vvw, GHSA-xpw8-rcwv-8f8p, CVE-2026-33871	≥ 4.1.132.Final

rails/rails

Repository: <https://github.com/rails/rails.git>

Version analysed: v8.1.3 (commit 2026-03-24) | ORT run: 2026-05-27

Dependencies: 499 packages (NPM: 499)

Vulnerabilities: 94 total — Critical: 5, High: 34, Medium: 50, Low: 5

Package	Sev.	Score	Advisories	Upgrade / Fix
flatted@3.3.1	Critical	9.8	CVE-2026-33228, GHSA-25h7-pfq9-p65f, GHSA-rf6f-7fwh-wjgh, CVE-2026-32141	≥ 3.4.0
tough-cookie@2.4.3	Critical	9.8	CVE-2023-26136, GHSA-72xf-g2v4-qvf3	≥ 4.1.3
form-data@2.3.3	Critical	9.4	GHSA-fjxv-7rqg-78g4, CVE-2025-7783	≥ 2.5.4
rollup@2.79.1	Critical	9.3	CVE-2026-27606, GHSA-mw96-cpmx-2vgc, GHSA-gcx4-mw62-g8wm, CVE-2024-47068	≥ 2.80.0
socket.io-parser@4.2.4	High	8.7	GHSA-677m-j7p3-52f9, CVE-2026-33151	≥ 3.3.5

3.7.2 Renowned Open Source Projects

The projects listed under section 2.2.1 were chosen since they host their source code on GitHub for easy comparison with [GitHub dependency insights](#) and [GitHub advanced security](#). The following presents key numbers on the analysis of each of them, based on the run status at the end of March 2026, with some updates in May 2026.

3.7.2.1 Hadoop



Hadoop (Git commit 4d78253)	ORT Server	GitHub	Remark
Dependencies	1677	4142	Difference is mostly due to the way of calculating the number of Maven dependencies
Bower	27	-	GitHub does not support Bower
NPM	1003	1787	Mismatch might be due to GitHub showing data for another revision
Python	21	1	GitHub does not get transitive dependencies
Maven	626	2347	GitHub counts Maven projects and plugins. While ORT Server covers Maven projects, the numbers are calculated differently.
GitHub Actions	-	7	ORT Server does not support analysis of GitHub Actions
Vulnerabilities	1103	-	GitHub advanced security not configured/not available

Conclusion: A failure during analysis of NuGet projects with ORT Server leads to no results for that ecosystem from ORT Server. GitHub omits all transitive dependencies of Python dependencies listed in a [requirements.txt](#) file, which might result in undetected vulnerabilities. GitHub lists more Maven packages as it also counts Maven sub-projects and Maven plugins as packages.

3.7.2.2 Kafka

Kafka (Git commit a35d649)	ORT Server	GitHub	Remark
Dependencies	96	74	ORT Server does not support analysis of GitHub Actions, but otherwise caught more dependencies.
Python	64	25	GitHub seems to not parse <code>~=</code> relations
Maven	32	10	GitHub seems to omit non-standard scope "swaggerDeps"
GitHub Actions	-	39	ORT Server does not support GitHub Actions



Vulnerabilities	51	-	GitHub advanced security not configured/not available
-----------------	----	---	---

Conclusion: With the exception of GitHub actions, which are not (yet) supported by ORT Server, the analysis by ORT Server draws a more complete picture including "compatible" Python dependencies declared with `~=` and Maven dependencies from non-standard scopes.

3.7.2.3 Tomcat

Tomcat commit 2c59450 (Git)	ORT Server	GitHub	Remark
Dependencies	40	51	ORT Server does not support analysis of GitHub Actions
Maven	40	40	
GitHub Actions	-	11	ORT Server does not support analysis of GitHub Actions
Vulnerabilities	45	-	GitHub advanced security not configured/not available

Conclusion: Again with the exception of GitHub actions, ORT Server and GitHub agree on the dependencies.

3.7.2.4 Mosquitto

Mosquitto commit b3b4d77 (Git)	ORT Server	GitHub	Remark
Dependencies	-	34	ORT Server does not support analysis of GitHub Actions
GitHub Actions	-	34	ORT Server does not support analysis of GitHub Actions
Vulnerabilities	0	-	GitHub advanced security not configured/not available

Conclusion: The project mostly uses C / C++ without a dedicated package manager, thus dependencies cannot be programmatically analyzed, neither by ORT Server nor by GitHub.



As a fallback, ORT Server provides means to manually declare dependencies in a machine-readable format, like SPDX.

3.7.2.5 Jetty

Jetty commit 8c218d9 (Git)	ORT Server	GitHub	Remark
Dependencies	725	5396	Difference is mostly due to the way of calculating the number of Maven dependencies
Maven	725	5390	ORT Server does not capture Maven plugins; GitHub treats project dependencies as packages
GitHub Actions	-	6	ORT Server does not support analysis of GitHub Actions
Vulnerabilities	104	-	GitHub advanced security not configured/not available

Conclusion:

- **ORT Server in general supports a wider set of technologies and supports better transitive dependency resolution when compared to GitHub**
- GitHub lists a lot more Maven dependency than ORT Server does. This is mainly due to two factors: 1. GitHub treats inter-dependencies between projects in a multi-project setup as packages. As the project has many (sub-)projects, this increases the number of packages a lot. 2. GitHub also lists plugins to the Maven build system as Maven dependencies. As these are build-time dependencies that are not distributed as part of the product, ORT Server currently disregards these.
- Github analyses its own GitHub Actions which the ORT Server does not.
- Using GitHub advanced security requires separate configuration and may require paid plans, depending on the case; these projects had not enabled that GitHub feature. ORT Server accesses vulnerability data from free data sources.

3.8 Planned Improvements

To address the noted current limitations, this lists the planned improvements until the end of the OCCTET project:

- [Allow more than just VCS repositories as input to create runs from](#)
- [Rework VulnerabilityResolutionReason for CRA / DORA requirements](#)
- [Extend the ORT advisor model with fixed version information](#)



-
- [Allow to automatically re-run jobs based on a schedule / event trigger](#)
 - [Integrate plugin manager with UI to trigger runs](#)
 - [Add a reporter for exploitable vulnerabilities in OpenVEX format](#)
 - General UX improvements, e.g. more efficient navigation in the UI for different use-cases
 - Ongoing bug fixes based on finding from this milestone deliverable and continuous dogfooding



4 Curator

4.1 Bitsea's role in OCCTET

Bitsea is a leading provider of software audits and sustainable open source security, risk, and compliance management. For more than a decade, well-known companies in the automotive, telecommunications, financial services, logistics, and aerospace sectors have relied on Bitsea's expertise—whether for technical due diligence during M&A activities or for supporting secure digital transformation.

As an active member of the OpenChain project, Bitsea combines deep legal-technical know-how with collaborative, partner-based innovation. Within the OCCTET project, Bitsea is responsible for designing and implementing key functionality related to automated license curation, metadata enrichment, and audit result validation. By building on its proven experience in FOSS compliance, Bitsea contributes to making OCCTET a robust, regulatory-aligned toolkit for the entire European software ecosystem.

The Bitsea OCCTET Curator is designed as a practical, AI-supported web application to streamline open source software auditing for SMEs and larger enterprises alike. It targets both license compliance and vulnerability management, responding directly to growing demands under the Cyber Resilience Act (CRA) and broader software supply chain obligations.

4.2 OCCTET Curator On GitHub

Occtet Curator is open source and can be downloaded at:
<https://github.com/Bitsea/Occtet-Curator>

Current tag: <https://github.com/Bitsea/Occtet-Curator/releases/tag/Toolkit-Demo-Del-D3.3>

4.3 Current Status

The current version is still in development and it will be finished as planned by Oct 31, 2026. The connection to the Federated Database of ABCD is established and functional. Integration with the ORT server is established and functional.

An AI is already integrated that already supports basic tasks. Features of vulnerability management have been implemented.

The current version remains under development and is scheduled for completion by October 30, 2026, as planned. The connection to the Federated Database of ABCD is established and operational. Integration with the ORT server is established and functional.

An Artificial Intelligence component has been integrated, providing support for basic tasks. Vulnerability management features have also been successfully implemented.

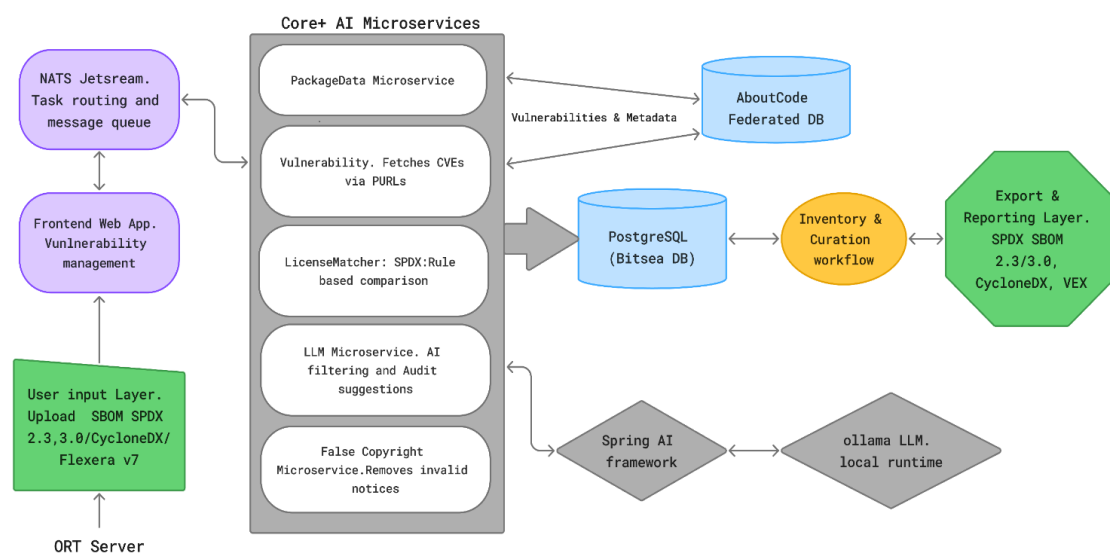


4.4 Installation

The installation is Docker-based and described in the readme in Github. The file "occtet-nats/docker-compose.yml" contains all necessary configurations (ports, password, paths, mappings). The Dockerfiles are built with "docker compose up".

4.5 Architecture

The following diagram shows the architecture:



The Bitsea OCCTET curator is designed as a modern web-based application with a modular microservices architecture, enabling scalable, maintainable, and highly customizable audit workflows. It combines a user-friendly frontend for inventory and report management with a robust backend that orchestrates multiple specialized services. The architecture reflects key design goals of audit traceability, interoperability, and AI-assisted decision support — aligned with the needs of small and medium-sized enterprises (SMEs) working towards secure open source usage and CRA compliance.

4.6 User Interface

The user experience is a web-based interface built using the Jmix (v2.6) framework, which extends Spring Boot to simplify the creation of enterprise-grade applications. The UI allows users to upload SBOMs and audit reports, configure scan parameters, view results, and manage open source software inventory items and their licenses and vulnerabilities.

Each task initiated in the frontend, such as uploading a Flexera FossReport or an SPDX SBOM, results in a configuration being generated and associated with a scanning job. This configuration is passed into the system via a well-defined process and can include file uploads, string-based values, or base paths, depending on the specific scan type.



The frontend also communicates asynchronously with backend services through a messaging queue system, which supports decoupled and scalable processing of long-running or computationally intensive tasks.

4.7 Microservices and Task Isolation

The tool follows a task-oriented microservices architecture, where each microservice is responsible for a single, clearly defined function in the audit pipeline. These microservices are implemented using Spring Boot and communicate using the NATS messaging system, which is configured in JetStream work queue mode to support reliable and distributed task execution.

When a task is initiated from the frontend, a corresponding message is published to a subject in the NATS stream. The appropriate microservice consumes this message, processes the data, and sends back results or error messages on a response subject. This pattern ensures scalability and clean separation of concerns.

Microservices include, among others:

- **SPDXMicroService:** Processes SPDX 2.3 SBOMs and extracts license, copyright, and component data.
- **VulnerabilityMicroService:** Looks up CVE data from external sources based on software component identifiers (e.g., PURLs).
- **DownloadMicroServices:** Allow generation of new SPDX SBOMs or FossReports from curated inventory.
- **LLMMicroService:** Uses local LLMs (via Ollama) for intelligent text analysis (e.g., false positive detection, license classification)
- **PackageDataMicroService:** Enriches metadata for packages via external registries (e.g., PURL-based)
- **DownloadSPDX/FossReport:** Generates new curated SBOMs
- **ControlSPDXMicroService:** Validates SBOM structure and consistency
- **InformationFileMicroService:** Processes custom information files for AI indexing and reference

Each microservice interacts with a common PostgreSQL database (v16.0), where curated audit entities (Vulnerabilities, InventoryItem, SoftwareComponent, License, Copyright, etc.) are stored.

4.8 Messaging Infrastructure: NATS and JetStream

The system uses NATS as its core messaging and streaming system. NATS is a CNCF-certified lightweight publish-subscribe system, which allows various services to communicate asynchronously without direct dependencies.

JetStream, NATS' persistence layer, is activated to support the work queue model, where each task is distributed reliably and durably to the appropriate microservice. Messages are stored in a dedicated location and can be pulled by multiple clients. While currently each task queue has a single consumer, the architecture supports load balancing and parallelism in future deployments.

This message-driven architecture ensures robust handling of task status, error propagation, and result delivery, while simplifying orchestration across services.



4.9 AI and Local Language Model Integration

To support intelligent automation in audit workflows, OCCTET Curator includes a dedicated AI microservice, which connects to locally hosted open source large language models via the Ollama framework. This allows sensitive code or information to be processed without relying on external cloud APIs, preserving data confidentiality and enabling offline deployment.

The AI microservice uses Spring AI for local model access and inference, and supports modular integration of additional tools such as:

- Autocomplete and text suggestion for curation fields,
- Copyright validation and filtering,
- License classification and deviation detection.

The system is also designed to support hybrid AI workflows, combining rule-based tools with retrieval-augmented generation (RAG) pipelines. These pipelines use document chunking, vector databases, and reranking techniques to improve the quality and relevance of AI responses.

4.10 External Data Sources and Enrichment

Several microservices are responsible for augmenting internal data with external metadata and vulnerability information. This includes:

- Querying third-party metadata databases like AboutCode, ClearlyDefined, and deps.dev,
- Fetching SBOM fragments and license texts from GitHub or SPDX.org,
- Contacting vulnerability databases via CVE or PURL identifiers.

The system is designed to support enrichment-on-demand, reducing the need for complete upfront data and supporting incremental curation.

4.11 Open Source Licensing and Sustainability

Bitsea OCCTET Curator is released as free and open source software under the Apache-2.0 license. The source code is publicly available on GitHub, allowing other audit providers, security teams, or compliance officers to reuse and adapt the toolkit for their own needs.

4.12 Deployment and Packaging

OCCTET Curator is designed for flexible deployment to accommodate the varying technical capacities of its users including small and medium-sized enterprises (SMEs). It can be deployed either as:

- A self-contained JAR file for each microservice and the frontend UI, using the standard Spring Boot build process,
- A project-wide Gradle build, enabling consistent compilation, dependency resolution, and artifact generation,
- Or as a Docker image, allowing easy containerization and orchestration using Docker Compose or Kubernetes.



For users familiar with container-based environments, each component of the Bitsea OCCTET Curator architecture from the NATS server and PostgreSQL database to the individual Spring Boot microservices can be encapsulated in a Docker image. This enables reproducible environments, versioned deployments, and simplified dependency management, which are especially beneficial in regulated or security-sensitive settings.

Pre-built Docker images may be provided for convenience, or users can generate them via the Gradle build pipeline. This approach supports both local development setups and production deployments in cloud or on-premise infrastructure.

4.13 Docker images

To support portability, reproducibility, and ease of setup, OCCTET Curator will be delivered as a set of 4 to 5 Docker images, each representing a core component of the system. These pre-built images package each microservice or service layer along with its required runtime environment, dependencies, and configuration.

The images are expected to include (tentatively)

- The Jmix-based frontend UI,
- One or more backend microservices (e.g., SPDX and FossReport processors),
- The AI microservice, which runs Spring AI integrated with locally hosted open models via Ollama,
- And optionally, utility components such as the NATS JetStream server or a database initializer.

This containerized architecture allows the tool to be deployed easily via Docker or Docker Compose, making it suitable for both local development and scalable production environments. The use of container images also facilitates compliance and reproducibility in regulated sectors.

4.14 Vulnerability Detection and CRA Alignment

Vulnerability Management via Software Bill of Materials (SBOM)

OCCTET curator supports both SPDX and CycloneDX SBOM formats and uses them to detect known vulnerabilities through component identifiers (such as PURLs). This information is matched against public vulnerability databases (like GitHub Advisory DB, NVD, etc.) to assess security risks. When scanner results contain missing or inaccurate metadata (such as license name, version, or source), the AI fills in the gaps based on past curated data, reducing manual work and improving accuracy.

CRA Readiness and SBOM Quality

While the CRA emphasizes vulnerability disclosure, OCCTET ensures the SBOM also meets broader industry expectations, including full licensing, authorship, and dependency traceability. This holistic approach supports organizations seeking CRA compliance and internal software governance at the same time.



4.15 VEX integration

The OCCTET Curator is designed not only to help users identify and manage vulnerabilities in open source components but also to support structured documentation of their exploitability status through VEX (Vulnerability Exploitability eXchange) integration. The Curator can generate VEX documents in formats aligned with SPDX 3.0 or CycloneDX standards, or prepare them as standalone machine-readable statements.

After all findings are curated, the project can export a new SBOM (in SPDX 2.3,3.0, CycloneDX) with validated and annotated vulnerability information. These exports fulfill the CRA requirement of maintaining accurate, up-to-date documentation of security-relevant components. Organizations can share these curated SBOMs with suppliers, customers, or regulators as part of their cybersecurity posture reporting.

4.16 Validation with SME data

The Small and Medium-sized Enterprise (SME) test data, as referenced in the chapter on test data, will be processed. The curator interacts with the ORT Server via an API to retrieve the scan results. This data will subsequently be displayed within the curator interface. All statistics derived from the ORT Server are equally applicable to the curator, as the Curator is dependent on the input provided by the ORT Server.

4.16.1 SME-Tester: ReductSoftware UG

Repositories:

- <https://github.com/reductstore/reduct-rs>
- <https://github.com/reductstore/reductstore>
- <https://github.com/reductstore/web-console>



The screenshot shows the 'Occtet Curator' application interface. The left sidebar contains navigation options: Dashboard, SBOM Mgmt, Vulnerabilities, VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and Administration. The main area is titled 'SBOM Mgmt' and shows the 'Overview' tab for the 'reduct-store - test' project. It lists 862 Copyrights, 44 Licenses, and 1 Vulnerability. A table shows the vulnerability details:

Vulnerability	Risk score of vulnerability	Number in software components
VCD-adtp-9da8-zua1	2.1	3

On the right, a detailed view of the vulnerability is shown, listing various items and their associated files. The items include various source artifacts and licenses, such as 'adler2.0.1-source-artifact', 'adler2.0.1-vcs', 'aes-0.6.6-rc-10-source-artifact', etc.

Figure: View the content of reduct-store with vulnerability

The screenshot shows the 'Occtet Curator' application interface. The left sidebar contains navigation options: Dashboard, SBOM Mgmt, Vulnerabilities, VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and Administration. The main area is titled 'Vulnerabilities' and shows the 'Overview' tab for the 'reduct-store - test' project. It displays a table of vulnerabilities:

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Last update
VCD-adtp-9da8-zua1	CVE-2024-4539, GHSA-5239-wwm-4pmq	4.3	0.5	2.1	http://public.vulnerabilitycode.io/vulnerabilities/VCD-adtp-9da8-zua1	03/06/2024 13:52:17:122

At the bottom, there are buttons for 'Edit' and 'Remove', and a 'Show all' button. The interface also includes a 'Filter' section and a '1 row' indicator.

Figure: Overview Vulnerabilities of reduct-store

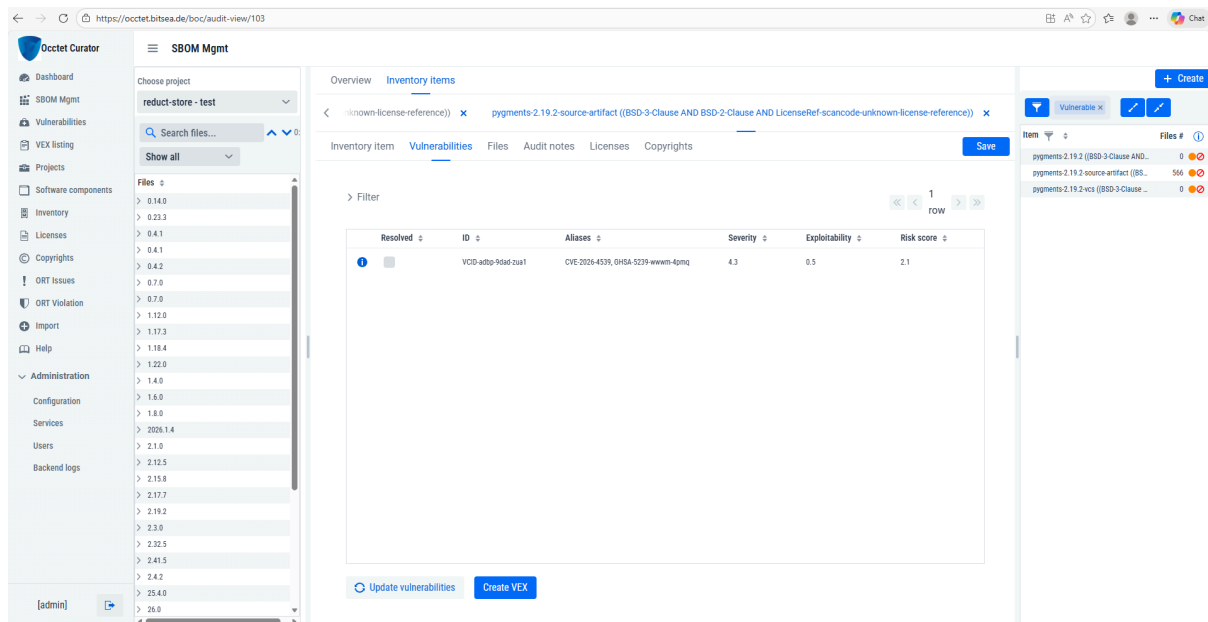


Figure: How to create a VEX

However, it is crucial to resolve the issues identified during the Scan. The following figure illustrates this issue, which stems from the Scan of <https://github.com/reductstore/reductstore>.

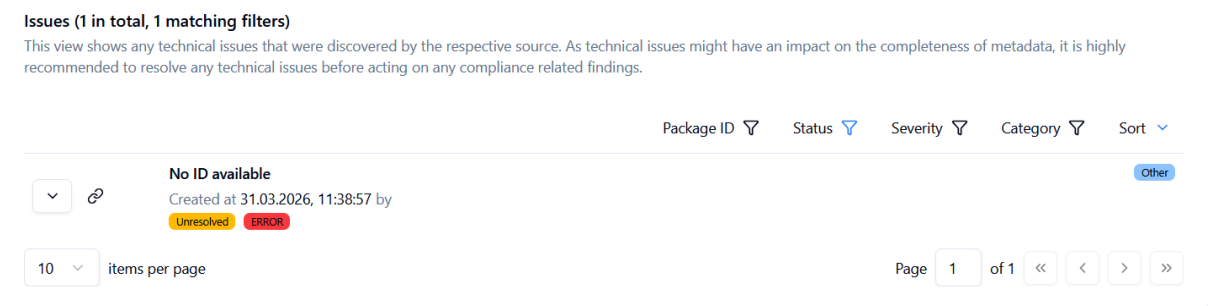
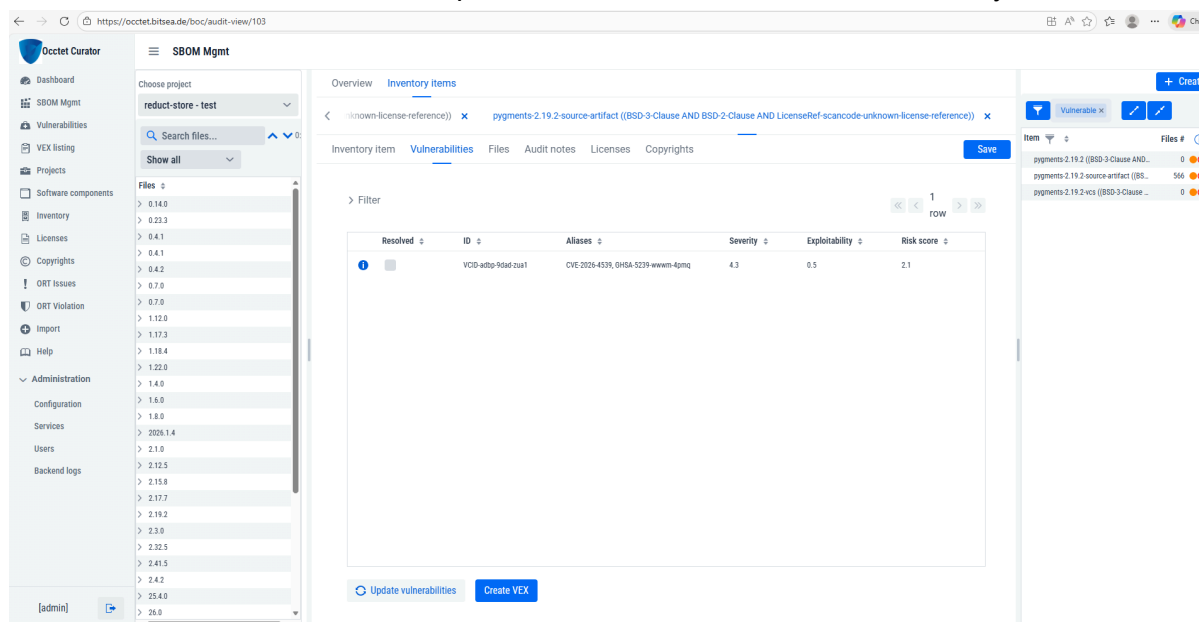
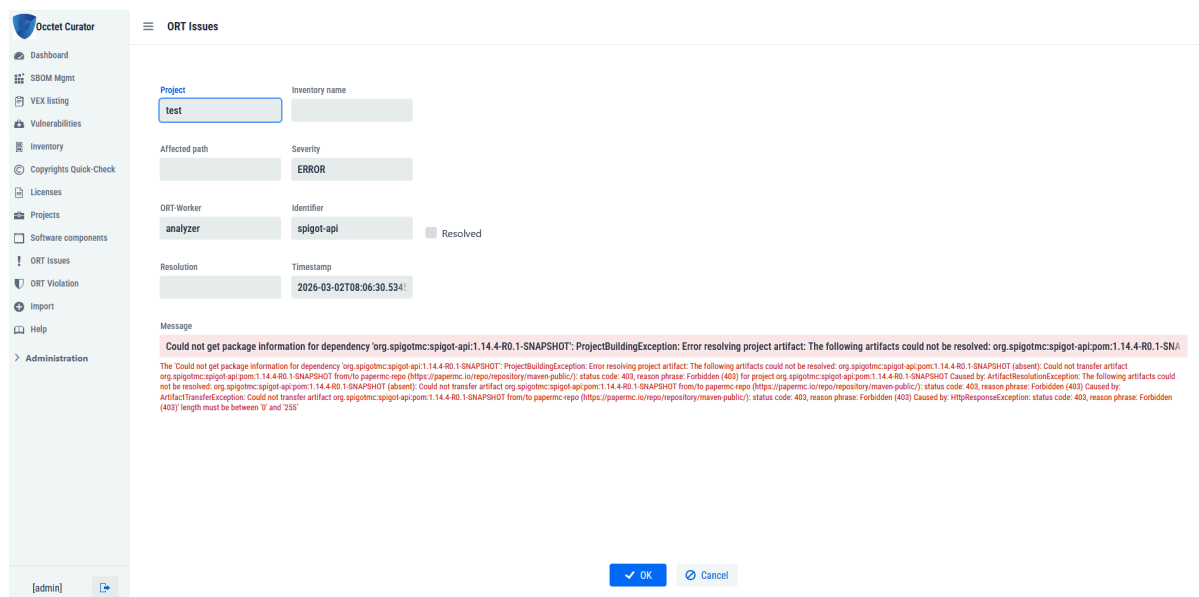


Figure from Scan of SME test data





https://occtet.bitsea.de/boc/projects

Occtet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities
- VEX listing
- Projects**
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration
 - Configuration
 - Services
 - Users
 - Backend logs

Projects

Filter

Refresh Add search condition

2 rows

Name	Version
reduct-rs	test
reduct-store	test

Export SBOM Export SBOM

+ Create Edit

[admin]

Validate Tomcat data:

https://occtet.bitsea.de/boc/software-components

Occtet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities
- VEX listing
- Projects
- Software components**
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration
 - Configuration
 - Services
 - Users
 - Backend logs

Software components

Choose project

tomcat - test Show all

Filter

46 rows

Name	Version	PURL	Licenses	Curated	License controlled by AI
tomcat-cxf	4.1.1		Zlib, CDDL-1.0, Apache-2.0, GPL-1.0, bzip2-1.0.6, EPL-1.0	False	
tomcat-jdbc	1.1.0-SNAPSHOT		Apache-2.0	False	
tomcat-owd	4.0.3		CDDL-1.0, CPL-1.0, Apache-2.0, EPL-2.0, Zlib, bzip2-1.0.6	False	
tomcat-stuffed	1.0		CDDL-1.0, CPL-1.0, Apache-2.0, EPL-2.0, Zlib, bzip2-1.0.6	False	
tomcat	db0c0baad609f2d4720953291b5c196c47380fe		EPL-2.0, CDDL-1.0, CDDL-1.0, LicenseRef-scancode-misc	False	
woodstox-core	7.1.0	pkg:maven/com.fasterxml/woodstox/woodstox-core@7.1.0	Apache-2.0	False	
h2	2.2.220	pkg:maven/com.h2database/h2@2.2.220	GPL-2.0-or-later, BSD-3-Clause, MPL-2.0, Unknown, L	False	
istack-commons-runtime	4.1.2	pkg:maven/com.sun.istack/istack-commons-runtime@4.1.2	BSD-3-Clause	False	
jakarta.activation-api	2.1.3	pkg:maven/jakarta.activation/jakarta.activation-api@2.1.3	Apache-2.0, GPL-2.0-only, BSD-3-Clause, EPL-2.0	False	
jakarta.annotation-api	2.1.0	pkg:maven/jakarta.annotation/jakarta.annotation-api@2.1.0	GPL-2.0-only, CDDL-1.0	False	
jakarta.annotation-api	2.1.1	pkg:maven/jakarta.annotation/jakarta.annotation-api@2.1.1	EPL-2.0, CDDL-1.0, GPL-2.0-only	False	
jakarta-el-api	5.0.0	pkg:maven/jakarta.el/jakarta.el-api@5.0.0	GPL-2.0-only, EPL-2.0, Unknown	False	
jakarta.enterprise-cdi-api	4.0.1	pkg:maven/jakarta.enterprise/jakarta.enterprise.cdi-api@4.0.1	Apache-2.0, Unknown, EPL-2.0	False	
jakarta.enterprise-lang-model	4.0.1	pkg:maven/jakarta.enterprise/jakarta.enterprise.lang-model@4.0.1	Apache-2.0, EPL-2.0, Unknown	False	
jakarta.inject-api	2.0.1	pkg:maven/jakarta.inject/jakarta.inject-api@2.0.1	BSD-3-Clause, Apache-2.0	False	
jakarta.json.bind-api	3.0.1	pkg:maven/jakarta.json.bind/jakarta.json.bind-api@3.0.1	GPL-2.0-only, EPL-2.0	False	
jakarta.ws.rs-api	3.1.0	pkg:maven/jakarta.ws.rs/jakarta.ws.rs-api@3.1.0	CPL-1.0, EPL-2.0, Apache-2.0, GPL-2.0-only, EPL-1.0	False	
jakarta.xml.bind-api	4.0.2	pkg:maven/jakarta.xml.bind/jakarta.xml.bind-api@4.0.2	BSD-3-Clause, Unknown	False	
junix	4.13.2	pkg:maven/junix/junix@4.13.2	EPL-1.0	False	
cxf-core	4.1.1	pkg:maven/org.apache.cxf/cxf-core@4.1.1	Apache-2.0	False	
cxf-integration-cdi	4.1.1	pkg:maven/org.apache.cxf/cxf-integration-cdi@4.1.1	Apache-2.0	False	
cxf-rt-client	4.1.1	pkg:maven/org.apache.cxf/cxf-rt-client@4.1.1	Apache-2.0	False	

+ Create Edit Remove

[admin]

Figure Components of Tomcat code



ID	Aliases	Severity	Exploitability	Risk score	Source URL	Last update
VCD-adtp-9dad-zua1	CVE-2024-4539, GHSA-5239-wwwn-4pmq	4.3	0.5	2.1	http://public.vulnerablecode.io/vulnerabilities/VCD-adtp-9dad-zua1	03/30/2024 13:52:17:122

Figure Vulnerability at Tomcat code

4.16.2 SME Tester: Obeo

Repository: <https://github.com/eclipse-sirius/sirius-web.git>

Result Stats from Curator:

Detected Components: 1148

Detected Vulnerabilities: 48

SBOM can be generated

4.17 Validation with OSS projects

The testing and validation of the OCCTET curator was conducted on a varied set of widely used OSS projects. This section will show the validation results of each tested OSS project and how the OCCTET curator analyzes.

4.17.1 projects

4.17.1.1 dotnet/runtime

<https://github.com/dotnet/runtime>

Figure Software components in dot-net-runtime code



SBOM Mgmt

Choose project

dot-net-runtime - 11.0.100

Search files...

Show all

Files

dependencies

actions create pull request

..test_

create or update branch int te...

entrypoint.sh

git-auth-helper.int.test.ts

integration-tests.sh

units.unit.test.ts

dist

bridge.js

events.js

index.js

setup-node-sandbox.js

setup-sandbox.js

docs

assets

concepts-guidelines.md

examples.md

updating.md

src

create or update branch.ts

create-pull-request.ts

git-auth-helper.ts

git-command-manager.ts

github-helper.ts

Overview

Inventory items

Inventory item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Inventory name

\src\native\external\libunwind\github\workflows\CI-unix.yml

Parent inventory item

Software component

\src\native\external\libunwind\github\workflows\CI-unix.yml

Download URL

Linking

Priority

Number of files

1

Curated

Created at: 04/14/2026 13:15:47:131

+ Create

Item

Files #

\src\mono\samples\wasf\co\package-loc...

1

\src\native\external\libunwind\github\w...

1

\src\native\external\libunwind\github\w...

1

\src\native\external\libunwind\github\w...

1

\src\native\external\libunwind\github\w...

1

\src\native\external\libunwind\scripts\w...

1

\src\native\package-lock.json

1

\src\tests\FunctionalTests\Android.Devic...

1

C-Users\Jithendra.Palapu\Downloads\run...

0

-2efed9b7644c2000.0.0.0 (NOASS...

0

microsoft-dotnet-runtime-05b17e18...

0

microsoft-dotnet-runtime-4ebd3efdc...

0

src-libraries\System.Private.Xml.test...

0

src-libraries\System.Private.Xml.test...

0

src-libraries\System.Reflection.Meta...

0

src-libraries\System.Reflection.Meta...

0

src-libraries\System.Reflection.Meta...

0

action-actions-locker-dc20fa9a39...

0

action-actions-checkout-0c36a6a6...

0

action-actions-checkout-4ebd3efdc...

0

action-actions-checkout-4e9896f1...

0

action-actions-checkout-3e646aef...

0

action-actions-checkout-979713123...

0

action-actions-checkout-bc8ba2c3...

0

action-actions-checkout-c9409ca6b...

0

action-actions-checkout-42907c449...

0

action-actions-checkout-e6962627...

0

localhost:8090/boc/vulnerabilities

Octet Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Vulnerabilities

Choose project

dot-net-runtime - 11.0.

ID

Aliases

Severity

Exploitability

Risk score

Source URL

Manually created

Last update

[admin]

+ Create

Edit

Remove

Excel

JSON

Figure Vulnerabilities view



4.17.1.2 Avalonia

<https://github.com/AvaloniaUI/Avalonia>

localhost:8090/boc/audit-view/102

SBOM Mgmt

Choose project
avalonia - 12.0.1

Search files... 0/0

Show all

Files

- dependencies
- checkouts
- v4
- licenses
- rpm
- gactions
- gfastify
- gocraft
- before-after-hook.dep.yml
- deprecation.dep.yml
- once.dep.yml
- semver.dep.yml
- tunnel.dep.yml
- undici.dep.yml
- universal-user-agent.dep...
- uid 3.4.0.dep.yml
- uid 3.3.2.dep.yml
- uid 9.0.1.dep.yml
- wrappy.dep.yml
- __test__
- ads
- dist
- images
- src
- .eslintignore
- .eslintrc.json

Overview

Copyrights (0)

Copyright name Number in files

Licenses (0)

Vulnerabilities (0)

Item Files #

- github/workflows/api-diff.yml 1
- github/workflows/CLA.yml 1
- github/workflows/update-api.yml 1
- C-Users\Jithendra Palepu\Downloads\Avalon...

+ Create

localhost:8090/boc/vulnerabilities

Vulnerabilities

Choose project
avalonia - 12.0.1

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

+ Create Edit Remove

Excel JSON



localhost:8090/boc/software-components

Software components

Choose project
avalonia - 12.0.1

> Filter

Name	Version	PURL	Licenses	Curated	License controlled by AI
.CLABot	UNKNOWN			False	
actions/checkout	v4	pkg:github/actions/checkout@v4		False	
actions/github-script	v7	pkg:github/actions/github-script@v7		False	
actions/setup-dotnet	v4	pkg:github/actions/setup-dotnet@v4		False	
C:\Users\Jithendra.Palapu\Downloads\Avalonia-12.0.1				False	
github/workflows/update-api.yml	Standalone			False	
github/workflows/CLA.yml	Standalone			False	
github/workflows/api-diff.yml	Standalone			False	

+ Create Edit Remove

localhost:8090/boc/inventory-items

Inventory

Choose project
avalonia - 12.0.1

> Filter

Inventory name	Software component	Size	Linking	Curated
github/workflows/update-api.yml	github/workflows/update-api.yml	1		False
action-actions-checkout-41e9c359cb03314 (NOASSERTION)	actions/checkout	0		False
action-actions-checkout-bbb0b090a7a7214 (NOASSERTION)	actions/checkout	0		False
action-actions-github-script-d13c12e88130e43v7 (NOASSERTION)	actions/github-script	0		False
action-actions-github-script-2bda958ee341b81v7 (NOASSERTION)	actions/github-script	0		False
action-actions-setup-dotnet-a71775ae01f0cf1744 (NOASSERTION)	actions/setup-dotnet	0		False
action-actions-setup-dotnet-15913272428737944 (NOASSERTION)	actions/setup-dotnet	0		False
action-.CLABot-59d95616400763a7UNKNOWN (NOASSERTION)	.CLABot	0		False
C:\Users\Jithendra.Palapu\Downloads\Avalonia-12.0.1 (NOASSERTION)	C:\Users\Jithendra.Palapu\Downloads\Avalonia-12.0.1	0		False
github/workflows/CLA.yml	github/workflows/CLA.yml	1		False
github/workflows/api-diff.yml	github/workflows/api-diff.yml	1		False

+ Create Edit Remove



4.17.1.3 Newtonsoft.Json

<https://github.com/JamesNK/Newtonsoft.Json>

The screenshot shows the SBOM Mgmt application interface. The top navigation bar includes a hamburger menu, the title "SBOM Mgmt", and user controls like "Anmelden" and "Chat". The main content area is divided into a left sidebar and a main panel. The sidebar shows a "Choose project" dropdown set to "newtonsoft - 13.0.4" and a "Files" section with a search bar and a list of files including dependencies, checkout, .4, licenses, .npm, .test, .ads, 0153-checkout-v2.md, dist, index.js, problem-matcher.json, images, test-ubuntu-glt.Dockerfile, test-ubuntu-glt.md, .ic, misc, ts-helper.ts, git-auth-helper.ts, git-command-manager.ts, git-directory-helper.ts, git-source-provider.ts, git-source-settings.ts, git-version.ts, github-api-helper.ts, input-helper.ts, and main.ts. The main panel has tabs for "Overview" and "Inventory Items". The "Overview" tab is active, showing sections for "Copyrights (0)", "Licenses (0)", and "Vulnerabilities (0)". A right sidebar shows a list of items with columns for "Item" and "Files #".

The screenshot shows the Vulnerabilities application interface. The top navigation bar includes a hamburger menu, the title "Vulnerabilities", and user controls like "Anmelden" and "Chat". The main content area is divided into a left sidebar and a main panel. The sidebar shows a "Choose project" dropdown set to "newtonsoft - 13.0.4". The main panel is a large empty table with columns: ID, Aliases, Severity, Exploitability, Risk score, Source URL, Manually created, and Last update. At the bottom of the interface, there are buttons for "+ Create", "Edit", "Remove", "Excel", and "JSON".



localhost:8090/boc/software-components

Software components

Choose project
newtonsoft - 13.0.4

> Filter

Name	Version	PURL	Licenses	Curated	License controlled by AI
actions/checkout	v4	pkg:github/actions/checkout@v4		False	
github/codeql-action/analyze	v3	pkg:github/github/codeql-action@v3#analyze		False	
github/codeql-action/init	v3	pkg:github/github/codeql-action@v3#init		False	
C:\Users\Jithendra.Palepu\Downloads\Newtonsoft.Json-13.0.0\Newtonsoft.Json-13.0.0.nupkg				False	
github/workflows/codeql.yml	Standalone			False	

5 rows

+ Create Edit Remove

4.17.1.4 Polly

<https://github.com/App-vNext/Polly>

localhost:8090/boc/audit-view/201

SBOM Mgmt

Choose project
polly - 5.6.0

Search files... 0.0

Show all

Files

Overview Inventory items

Copyrights (0)

Copyright name	Number in files
----------------	-----------------

Licenses (0)

Vulnerabilities (0)

+ Create

Item Files #

C:\Users\Jithendra.Palepu\Downloads\Polly-5.6.0\bin\Debug\net6.0\Polly.dll



localhost:8090/boc/vulnerabilities

Vulnerabilities

Choose project
polly - 5.6.0

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

+ Create Edit Remove

Excel JSON

localhost:8090/boc/software-components

Software components

Choose project
polly - 5.6.0

> Filter

Name	Version	PURL	Licenses	Curated	License controlled by AI
C:\Users\jithendra.Pakpu\Downloads\Polly-5.6.0.zip	sha256:f5af946346346f6ee859d72be432942efb1c1265478d0...			False	

<< < 1 row > >>

+ Create Edit Remove



4.17.1.5 Restsharp

<https://github.com/restsharp/RestSharp>

localhost:8090/boc/vulnerabilities

Vulnerabilities

Choose project
restsharp - 103.1

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

+ Create Edit Remove

Excel JSON

localhost:8090/boc/software-components

Software components

Choose project
restsharp - 103.1

> Filter

7 rows

Name	Version	PURL	Licenses	Curated	License controlled by AI
Newtonsoft.Json.NET	4.0.0.0	pkg:nugget/Newtonsoft.Json.NET@4.0.0.0		False	
NuGet	1.7.30402.9028	pkg:nugget/NuGet@1.7.30402.9028		False	
C:\Users\Jithendra.Palepu\Downloads\RestSharp-103.1				False	
\\References\Newtonsoft.Json.MonoTouch.dll	Standalone			False	
\\Tools\NuGet.exe	Standalone			False	
\\References\Newtonsoft.Json.MonoDroid.dll	Standalone			False	
\\nugget\NuGet.exe	Standalone			False	

+ Create Edit Remove



localhost:8090/boc/inventory-items

Inventory

Choose project
restsharp - 103.1

> Filter

Inventory name	Software component	Size	Linking	Curated
Newtonsoft.Json.NET.7.0.0.166c54.0.0.0 (NOASSERTION)	Newtonsoft.Json.NET	0		False
Newtonsoft.Json.NET.7.0.0.166c54.0.0.0 (NOASSERTION)	Newtonsoft.Json.NET	0		False
NuGet.8941a2177dea0bce1.7.30402.9028 (NOASSERTION)	NuGet	0		False
NuGet.780a5531ed72921.7.30402.9028 (NOASSERTION)	NuGet	0		False
C:\Users\jithendra.Palepu\Downloads\RestSharp.103.1 (NOASSERTION)	C:\Users\jithendra.Palepu\Downloads\RestSharp.103.1	0		False
V:\References\Newtonsoft.Json.MonoTouch.dll	V:\References\Newtonsoft.Json.MonoTouch.dll	1		False
V:\Tools\NuGet.exe	V:\Tools\NuGet.exe	1		False
V:\References\Newtonsoft.Json.MonoDroid.dll	V:\References\Newtonsoft.Json.MonoDroid.dll	1		False
V:\nuget\NuGet.exe	V:\nuget\NuGet.exe	1		False

9 ROWS

+ Create Edit Remove

localhost:8090/boc/audit-view/205

SBOM Mgmt

Choose project
restsharp - 103.1

Search files... 0/0

Show all

Files

Overview

Copyrights (0)

Copyright name	Number in files
----------------	-----------------

Licenses (0)

Vulnerabilities (0)

+ Create

Item	Files #
V:\nuget\NuGet.exe	1
V:\References\Newtonsoft.Json.MonoDroid.dll	1
V:\References\Newtonsoft.Json.MonoTouch.dll	1
V:\Tools\NuGet.exe	1
C:\Users\jithendra.Palepu\Downloads\RestSharp.103.1	0



4.17.1.6 Dapper

<https://github.com/DapperLib/Dapper>

localhost:8090/boc/audit-view/204

SBOM Mgmt

Choose project
dapper - 2.1.72

Search files... 0/0

Show all

Files

- dependencies
 - checklist
 - Y1
 - action.yml
 - CHANGELOG.md
 - LICENSE
 - README.md
 - github-action
 - Y2.3.0
 - main.test.ts
 - pullRequestLock.test.ts
 - dist
 - index.js
 - docs
 - images
 - adding-clafile.gif
 - allowlist.gif
 - personal-access-token.gif
 - personalaccess.token.gif
 - signature-process.gif
 - signature-storage-file.gif
 - src
 - persistence
 - persistence.ts
 - pullrequest

Overview

Copyrights (0)

Copyright name Number in files

Licenses (0)

Vulnerabilities (0)

Item Files #

- github/workflows/ci.yml 1
- github/workflows/main.yml 1
- C:\Users\Jithendra\Downloads\Dapper... 0

+ Create

localhost:8090/boc/vulnerabilities

Vulnerabilities

Choose project
dapper - 2.1.72

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

+ Create Edit Remove

Excel JSON



localhost:8090/boc/software-components

Anmelden

Chat

Software components

Choose project
dapper - 2.1.72

> Filter

<< 6 rows >>

Name	Version	PURL	Licenses	Curated	License controlled by AI
actions/setup-dotnet	v4	pkg:github/actions/setup-dotnet@v4		False	
actions/checkout	v1	pkg:github/actions/checkout@v1		False	
contributor-assistant/github-action	v2.3.0	pkg:github/contributor-assistant/github-action@v2.3.0		False	
C:\Users\Jithendra.Palepu\Downloads\Dapper-2.1.72				False	
\\github\workflows\main.yml	Standalone			False	
\\github\workflows\cia.yml	Standalone			False	

+ Create

Edit

Remove

localhost:8090/boc/inventory-items

Anmelden

Chat

Inventory

Choose project
dapper - 2.1.72

> Filter

<< 6 rows >>

Inventory name	Software component	Size	Linking	Curated
action-actions-setup-dotnet-006d0204fa30f8644 (NOASSERTION)	actions/setup-dotnet	0		False
action-actions-checkout-71sta54ce4eaa0dc1 (NOASSERTION)	actions/checkout	0		False
action-contributor-assistant-github-action-4a6c9254d476a1v2.3.0 (NOAS...	contributor-assistant/github-action	0		False
C:\Users\Jithendra.Palepu\Downloads\Dapper-2.1.72 (NOASSERTION)	C:\Users\Jithendra.Palepu\Downloads\Dapper-2.1.72	0		False
\\github\workflows\main.yml	\\github\workflows\main.yml	1		False
\\github\workflows\cia.yml	\\github\workflows\cia.yml	1		False

+ Create

Edit

Remove



4.17.1.7 Fluent validation

<https://github.com/FluentValidation/FluentValidation>

localhost:8090/boc/audit-view/203

SBOM Mgmt

Choose project
fluentValidation - 12.1.1

Search files... 0.0

Show all

Files

- dependencies
 - checkout
 - v2
 - licenses
 - rgm
 - __test__
 - git-auth-helper.test.ts
 - git-directory-helper.test.ts
 - git-version.test.ts
 - input-helper.test.ts
 - modify-work-tree.sh
 - override-git-version.cmd
 - override-git-version.sh
 - ref-helper.test.ts
 - retry-helper.test.ts
 - verify-basic.sh
 - verify-clean.sh
 - verify-ifs.sh
 - verify-no-unstaged-changes.sh
 - verify-side-by-side.sh
 - verify-submodules-false.sh
 - verify-submodules-recursive.sh
 - verify-submodules-true.sh
 - adrs
 - 0153-checkout-v2.md
 - dist

Overview

Copyrights (0)

Copyright name	Number in files
----------------	-----------------

Licenses (0)

Vulnerabilities (0)

Item Files #

\\github\workflows\ci.yml	1
\\github\workflows\lock.yml	1
\\docs\requirements.txt	1
\\docs\requirements.txt	1
C:\Users\Jithendra.Palpu\Downloads\Fluent...	0

+ Create

localhost:8090/boc/vulnerabilities

Vulnerabilities

Choose project
fluentValidation - 12.1.1

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

+ Create Edit Remove

Excel JSON



Software components

Choose project

fluentValidation - 12.1.

> Filter

16 rows

Name	Version	PURL	Licenses	Curated	License controlled by AI
actions/checkout	v2	pkg:github/actions/checkout@v2		False	
actions/setup-dotnet	v2	pkg:github/actions/setup-dotnet@v2		False	
alabaster	0.7.13	pkg:pypi/alabaster@0.7.13		False	
commonmark	0.9.1	pkg:pypi/commonmark@0.9.1		False	
dessant/lock-threads	v2	pkg:github/dessant/lock-threads@v2		False	
docutils	0.17	pkg:pypi/docutils@0.17		False	
mock	1.0.1	pkg:pypi/mock@1.0.1		False	
recommonmark	0.5.0	pkg:pypi/recommonmark@0.5.0		False	
sphinx	1.8.5	pkg:pypi/sphinx@1.8.5		False	
sphinx-autobuild	0.7.1	pkg:pypi/sphinx-autobuild@0.7.1		False	
sphinx-rtd-theme	0.4.3	pkg:pypi/sphinx-rtd-theme@0.4.3		False	
C:\Users\Jithendra.Palepu\Downloads\FluentValidation-12.1.1				False	
l:\github\workflows\lock.yml	Standalone			False	
l:\github\workflows\ci.yml	Standalone			False	
l\docs\requirements_rtd.txt	Standalone			False	
l\docs\requirements.txt	Standalone			False	

+ Create Edit Remove

Inventory

Choose project

fluentValidation - 12.1.

> Filter

16 rows

Inventory name	Software component	Size	Linking	Curated
action-actions-checkout-cb6dc621e997b0292 (NOASSERTION)	actions/checkout	0		False
action-actions-setup-dotnet-e5b0272211a1d06v2 (NOASSERTION)	actions/setup-dotnet	0		False
sphinx-autobuild-8683c768996146600.7.1 (NOASSERTION)	sphinx-autobuild	0		False
sphinx-rtd-theme-93a7822c6d9790.4.3 (NOASSERTION)	sphinx-rtd-theme	0		False
action-dessant-lock-threads-09005249c36b01b7v2 (NOASSERTION)	dessant/lock-threads	0		False
C:\Users\Jithendra.Palepu\Downloads\FluentValidation-12.1.1 (NOASSERTION)	C:\Users\Jithendra.Palepu\Downloads\FluentValidation-12.1.1	0		False
l:\github\workflows\lock.yml	l:\github\workflows\lock.yml	1		False
l:\github\workflows\ci.yml	l:\github\workflows\ci.yml	1		False
l\docs\requirements_rtd.txt	l\docs\requirements_rtd.txt	1		False
alabaster-71a8b99913cc98a07.13 (NOASSERTION)	alabaster	0		False
commonmark-c862d416cd993510.9.1 (NOASSERTION)	commonmark	0		False
docutils-b4d74c3360c45670.17 (NOASSERTION)	docutils	0		False
mock-c352bc9f5d8f5791.0.1 (NOASSERTION)	mock	0		False
recommonmark-b4766974f3a4365.5.0 (NOASSERTION)	recommonmark	0		False
sphinx-8763a9e301a2b6c1.8.5 (NOASSERTION)	sphinx	0		False
l\docs\requirements.txt	l\docs\requirements.txt	1		False

+ Create Edit Remove



4.17.1.8 Automapper

<https://github.com/AutoMapper/AutoMapper>

Item	Files #
AutoMapper-main-8c548b (NOASSERTION)	0
1.15.0-75c946 (MIT)	0
10.0.0-75c946 (MIT)	0
17.11.1-75c946 (MIT)	0
2.8.2-75c946 (Apache-2.0)	0
2.9.2-75c946 (Apache-2.0)	0
4.2.1-75c946 (BSD-3-Clause)	0
4.8.1-75c946 (MIT)	0
6.0.0-75c946 (Apache-2.0)	0
7.1.2-75c946 (BSD-3-Clause AND)	0
75c946 (NOASSERTION)	0
checkout-4-75c946 ** (NOAS...	0
checkout-4.2.0-75c946 (NOASSE...	0
lock-threads-5-75c946 ** (NO...	0
login-2-75c946 ** (NOASSE...	0
parser-2.0.0-75c946 (MIT)	0
rd-schema-1.3.0-75c946 (MIT)	0
setup-docker-4-75c946 ** (N...	0
test-reporter-1-75c946 ** (N...	0
upload-artifact-4-75c946 ** (L...	0

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update



OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Software components

Choose project

Auto Mapper - 1.0

> Filter

Name	Version	PURL	Licenses	Curated	License controlled by AI
xunit.runner.visualstudio	2.8.2	pkg:nugget/xunit.runner.visualstudio@2.8.2	Apache 2.0	False	
dessant/lock-threads	5.*	pkg:githubactions/dessant/lock-threads@5.%2A.%2A		False	
actions/checkout	4.*	pkg:githubactions/actions/checkout@4.%2A.%2A		False	
sphinx	7.1.2	pkg:pypi/sphinx@7.1.2	BSD-3 Clause, BSD-2 Clause	False	
sphinx-rtd-theme	1.3.0rc1	pkg:pypi/sphinx-rtd-theme@1.3.0rc1	MIT	False	
myst-parser	2.0.0	pkg:pypi/myst-parser@2.0.0	MIT	False	
System.Reflection.Emit		pkg:nugget/System.Reflection.Emit		False	
MinVer	6.0.0	pkg:nugget/MinVer@6.0.0	Apache 2.0	False	
PolySharp	1.15.0	pkg:nugget/PolySharp@1.15.0	MIT	False	
Microsoft.Extensions.DependencyInjection	10.0.0	pkg:nugget/Microsoft.Extensions.DependencyInjection	MIT	False	
Shouldly	4.2.1	pkg:nugget/Shouldly@4.2.1	BSD-2 Clause	False	
Microsoft.NET.Test.Sdk	17.11.1	pkg:nugget/Microsoft.NET.Test.Sdk@17.11.1	MIT	False	
xunit	2.9.2	pkg:nugget/xunit@2.9.2	Apache 2.0	False	
Testcontainers.MsSql	4.8.1	pkg:nugget/Testcontainers.MsSql@4.8.1	MIT	False	
dorny/test-reporter	1.*	pkg:githubactions/dorny/test-reporter@1.%2A.%2A		False	
azure/regex	2.*	pkg:githubactions/azure/regex@2.%2A.%2A		False	
actions/checkout	4.2.0	pkg:githubactions/actions/checkout@4.2.0		False	
actions/upload-artifact	4.*	pkg:githubactions/actions/upload-artifact@4.%2A.%2A		False	
actions/setup-dotnet	4.*	pkg:githubactions/actions/setup-dotnet@4.%2A.%2A		False	
com.github.LuckyPennySoftware/AutoMapper	main	pkg:github/LuckyPennySoftware/AutoMapper/main		False	

+ Create

Edit

Remove

4.17.1.9 Serilog

<https://github.com/serilog/serilog>

OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Software components

Choose project

serilog - 2234

> Filter

Name	Version	PURL	Licenses	Curated	License controlled by AI
xunit.runner.visualstudio	2.8.2	pkg:nugget/xunit.runner.visualstudio@2.8.2	Apache 2.0	False	
System.ValueTuple	4.5.0	pkg:nugget/System.ValueTuple@4.5.0	MIT	False	
PolySharp	1.15.0	pkg:nugget/PolySharp@1.15.0	MIT	False	
Shouldly	4.2.1	pkg:nugget/Shouldly@4.2.1	BSD-2 Clause	False	
Microsoft.NET.Test.Sdk	17.11.1	pkg:nugget/Microsoft.NET.Test.Sdk@17.11.1	MIT	False	
xunit	2.9.2	pkg:nugget/xunit@2.9.2	Apache 2.0	False	
PublicApiGenerator	11.1.0	pkg:nugget/PublicApiGenerator@11.1.0	MIT	False	
PolySharp	1.14.1	pkg:nugget/PolySharp@1.14.1	MIT	False	
BenchmarkDotNet	0.15.2	pkg:nugget/BenchmarkDotNet@0.15.2	MIT	False	
System.Formats.Asn1	9.0.0	pkg:nugget/System.Formats.Asn1@9.0.0	MIT	False	
System.ServiceModel.Http	8.1.0	pkg:nugget/System.ServiceModel.Http@8.1.0	MIT	False	
Newtonsoft.Json	13.0.3	pkg:nugget/Newtonsoft.Json@13.0.3	MIT	False	
System.ServiceModel.Http	4.10.3	pkg:nugget/System.ServiceModel.Http@4.10.3	MIT	False	
actions/setup-dotnet	5.*	pkg:githubactions/actions/setup-dotnet@5.%2A.%2A		False	
actions/checkout	5.*	pkg:githubactions/actions/checkout@5.%2A.%2A		False	
System.Threading.Channels	8.0.0	pkg:nugget/System.Threading.Channels@8.0.0	MIT	False	
System.Diagnostics.DiagnosticSource	8.0.1	pkg:nugget/System.Diagnostics.DiagnosticSource@8.0.1	MIT	False	
com.github.serilog/serilog	dev	pkg:github/serilog/serilog/dev	Apache 2.0	False	

+ Create

Edit

Remove



Octet Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

[admin]

SBOM Mgmt

Choose project

serilog - 2234

Search files...

Show all

Files

serilog

assets

serilog ank

serilog avg

results

net4.5.2

MessageTemplateCache

MessageTemplateCacheBenchmark_Cached-report-github...

MessageTemplateCacheBenchmark_Leaking-report-github...

LevelControlBenchmark-report-github.md

LogContextEnrichmentBenchmark-report-github.md

MessageTemplateParsingBenchmark-report-github.md

NestedLoggerCreationBenchmark-report-github.md

NestedLoggerLatencyBenchmark-report-github.md

PipelineBenchmark-report-github.md

net46

AllocationsBenchmark-report-github.md

netcoreapp1.0

MessageTemplateCache

MessageTemplateCacheBenchmark_Cached-report-github...

MessageTemplateCacheBenchmark_Leaking-report-github...

LevelControlBenchmark-report-github.md

LogContextEnrichmentBenchmark-report-github.md

MessageTemplateParsingBenchmark-report-github.md

Microsoft.AspNetCore.Mvc.RazorPages-report-github.md

Overview

Copyrights (0)

Licenses (3)

License	Number in software components
BSD-2-Clause	1
Apache 2.0	3
MIT	12

Vulnerabilities (0)

+ Create

Item	Files #
serilog-dev-285190 (Apache-2.0)	0
0.15.2-75c946 (MIT)	0
1.14.1-75c946 (MIT)	0
1.15.0-75c946 (MIT)	0
11.1.0-75c946 (MIT)	0
13.0.3-75c946 (MIT)	0
17.11.1-75c946 (MIT)	0
2.8.2-75c946 (Apache-2.0)	0
2.9.2-75c946 (Apache-2.0)	0
4.10.3-75c946 (MIT)	0
4.2.1-75c946 (BSD-2-Clause)	0
4.5.0-75c946 (MIT)	0
8.0.0-75c946 (MIT)	0
8.0.1-75c946 (MIT)	0
8.1.0-75c946 (MIT)	0
9.0.0-75c946 (MIT)	0
checkout5-75c9465 ** (NOAS...	0
setup-dotnet5-75c9465 ** (N...	0

Octet Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

[admin]

Vulnerabilities

Choose project

serilog - 2234

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

+ Create

Edit

Remove

Excel

JSON

OCCTET Deliverable Number: D 3.3 - SME Toolkit-Demo-Del - page 74



4.17.1.10 NLog:

<https://github.com/NLog/NLog>



Occet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities**
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration

Vulnerabilities

Choose project
NLog - 1.0

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

[admin] [Create] [Edit] [Remove] [Excel] [JSON]

4.17.2 Iconic Projects

4.17.2.1 Adoptium

openJDK 27-17 <https://dash.adoptium.net/trends>

<https://occtet.bitsea.de/boc/audit-view/302>

Occet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration

SBOM Mgmt

Choose project
OPENJDK-Eclipse-Adoptium

Search files...
Show all

Files

- dependencies
 - cache
 - devcontainer
 - dist
 - restore
 - index.js
 - restore-only
 - index.js
 - save
 - index.js
 - save-only
 - index.js
 - licenses
 - npm
 - @actions
 - @azure
 - @protobuf
 - @typespec
 - agent-bas
 - balanced
 - brace-exp
 - concat-ma
 - debug-dep
 - events-de

Overview

 - Copyrights (0)
 - Licenses (1)
 - Vulnerabilities (0)

Item Files #

action-actions-uploa-artifact-7487c313c5404e46v6 (NOASSERTION)	0
action-actions-uploa-artifact-956116950db172c6 (NOASSERTION)	0
action-github-actions-build-prog-62c78eedea702da (UNKNOWN)	0
action-github-actions-config-Rc1722a50bba420 (UNKNOWN)	0
action-github-actions-config-f13305444439b7 (UNKNOWN)	0
action-github-actions-config-falc7f73afbae5 (UNKNOWN)	0
action-github-actions-config-f4c044014e01579 (UNKNOWN)	0
action-github-actions-de-build-1107c51c08054c (UNKNOWN)	0
action-github-actions-de-build-369e100905f530 (UNKNOWN)	0
action-github-actions-de-build-a3ac9e2255a8c0 (UNKNOWN)	0
action-github-actions-de-build-d15ec0ab3070ba (UNKNOWN)	0
action-github-actions-de-build-eb7050399f982 (UNKNOWN)	0
action-github-actions-get-boogja-312d1173e99030 (UNKNOWN)	0
action-github-actions-get-boogja-3c4ec55a8b7eadd (UNKNOWN)	0
action-github-actions-get-boogja-59225338c9f22da (UNKNOWN)	0
action-github-actions-get-boogja-59e495a230529f9a (UNKNOWN)	0
action-github-actions-get-boogja-afc3d8138090c7f9c (UNKNOWN)	0
action-github-actions-get-boogja-6548c7f485901508 (UNKNOWN)	0
action-github-actions-get-bundles-c897a8094c7c523 (UNKNOWN)	0
action-github-actions-get-guest-51a719d39d909763 (UNKNOWN)	0
action-github-actions-get-guest-5f5564c19762c19 (UNKNOWN)	0
action-github-actions-get-guest-caab10010164345 (UNKNOWN)	0
action-github-actions-get-guest-f5449a719c7c04 (UNKNOWN)	0
action-github-actions-get-jreg-0a38994d7f9f456e (UNKNOWN)	0
action-github-actions-get-jreg-0e1056fede3a2 (UNKNOWN)	0
action-github-actions-get-jreg-7a0f50915da30 (UNKNOWN)	0
action-github-actions-get-jreg-a92cd70429a0303 (UNKNOWN)	0
action-github-actions-get-may2-91a55509e2e60997 (UNKNOWN)	0
action-github-actions-get-may2-95532a0a113a0c (UNKNOWN)	0

[curator-admin] [Create]



https://occtet.bitsea.de/boc/audit-view/205

Occtet Curator

SBOM Mgmt

Choose project: eclipse-ide - test

Search files...

Show all

Overview

> Copyrights (6)

> Licenses (52)

> Vulnerabilities (7)

Vulnerability	Risk score of vulnerability	Number in software components
VCD-4482-un5j-8fp	2.2	1
VCD-305j-8fyu-1qft	3.1	1
VCD-9761-y885-aaag	3.1	1
VCD-pu9y-153k-aaag	3.4	1
VCD-7yt5-z5e6-aaaa	4.5	1
VCD-z8en-jh3-aaag	4.5	2
VCD-j489-wp27-aaap	4	1

Files

C-Users.Jithendra.Palappu.Videos... 0

ApiSet Stub DLL 03b10e0540... 0

ApiSet Stub DLL 06744dc54a... 0

ApiSet Stub DLL 06c8e8177f... 0

ApiSet Stub DLL 07ebaf9063... 0

ApiSet Stub DLL 0809c86e32... 0

ApiSet Stub DLL 0d0f514b40... 0

ApiSet Stub DLL 0c44ace17... 0

ApiSet Stub DLL 18ea312c8... 0

ApiSet Stub DLL 1c5226ec50... 0

ApiSet Stub DLL 229c4bd50c... 0

ApiSet Stub DLL 2b224d9992... 0

ApiSet Stub DLL 4b35640106... 0

ApiSet Stub DLL 50558d344d... 0

ApiSet Stub DLL 619e3942c... 0

ApiSet Stub DLL 6d0dae66c... 0

ApiSet Stub DLL 7936a09e19... 0

ApiSet Stub DLL 7e73e7zdc9... 0

ApiSet Stub DLL 85198b3730... 0

ApiSet Stub DLL 91607db1ad... 0

ApiSet Stub DLL 9301e55839... 0

ApiSet Stub DLL 94042e86cd... 0

ApiSet Stub DLL 9c5c01e1a... 0

ApiSet Stub DLL a45b4c7f04... 0

ApiSet Stub DLL 02406a0a02... 0

ApiSet Stub DLL 027a07f9f4... 0

ApiSet Stub DLL 0b025c9c9... 0

ApiSet Stub DLL 0c24401c53... 0

https://occtet.bitsea.de/boc/audit-view/205

Occtet Curator

SBOM Mgmt

Choose project: eclipse-ide - test

Search files...

Show all

Overview

> Copyrights (6)

> Licenses (52)

> Vulnerabilities (7)

Vulnerability	Risk score of vulnerability	Number in software components
VCD-4482-un5j-8fp	2.2	1
VCD-305j-8fyu-1qft	3.1	1
VCD-9761-y885-aaag	3.1	1
VCD-pu9y-153k-aaag	3.4	1
VCD-7yt5-z5e6-aaaa	4.5	1
VCD-z8en-jh3-aaag	4.5	2
VCD-j489-wp27-aaap	4	1

Vulnerable

archive-commons-lang3-9e7d023ad0434623.4 (NOASSERTION) 0

archive-guava-8f52c172b1caaf12UNKNOWN (NOASSERTION) 0

archive-jansi-da836c529d1ad887UNKNOWN (NOASSERTION) 0

archive-joup-6c3d6050a279db1.14.2 (LicenseRef The MIT License) 0

archive-logback-core-1754e7c24313ec291.5.18 (NOASSERTION) 0

archive-maven-compat-d8e9f8d30270bdaUNKNOWN (NOASSERTION) 0

archive-maven-core-0fb630c356622UNKNOWN (NOASSERTION) 0



Octet Curator

Dashboard SBOM Mgmt Vulnerabilities VEX listing Projects Software components Inventory Licenses Copyrights ORT Issues ORT Violation Import Help Administration

Vulnerabilities

Choose project
eclipse-ide - test Show all

> Filter

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Last update
VCD-3qjnyh1ght	CVE-2025-48924, GHSA-288-qh7-25v	6.2	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VCD-3qjnyh1ght	04/07/2026 08:58:22.244
VCD-v48tz-un5j8ftp	CVE-2026-12225, GHSA-qppp-mvqg-44fv	4.5	0.5	2.2	http://public.vulnerablecode.io/vulnerabilities/VCD-v48tz-un5j8ftp	04/07/2026 08:59:44.751
VCD-7y5t5-25e6-aaaa	CVE-2020-8908, GHSA-5ng9-w23w-74m3	9	0.5	4.5	http://public.vulnerablecode.io/vulnerabilities/VCD-7y5t5-25e6-aaaa	04/07/2026 10:46:50.660
VCD-pu7fy-113k-aaag	CVE-2023-2976, GHSA-7q45-4m6-3mnc	6.8	0.5	3.4	http://public.vulnerablecode.io/vulnerabilities/VCD-pu7fy-113k-aaag	04/07/2026 10:46:50.700
VCD-s8en-qh3-aaag	CVE-2021-26291, GHSA-2t88-5hg8-9h2x	9	0.5	4.5	http://public.vulnerablecode.io/vulnerabilities/VCD-s8en-qh3-aaag	04/07/2026 11:19:29.339
VCD-j48w-wp27-aaag	CVE-2013-2035, GHSA-49j7-qgtp-5eij	8	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCD-j48w-wp27-aaag	04/07/2026 11:32:12.402
VCD-9761-y885-aaag	CVE-2022-36033, GHSA-gp7t-rwcv-9369	6.2	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VCD-9761-y885-aaag	04/08/2026 10:54:52.807

[admin] Edit Remove Excel JSON

Octet Curator

Dashboard SBOM Mgmt Vulnerabilities VEX listing Projects Software components Inventory Licenses Copyrights ORT Issues ORT Violation Import Help Administration

SBOM Mgmt

Choose project
eclipse-ide - test

Search files... Show all

Files

Overview Inventory items

archive-commons-lang3-9e7d3023abf434d23.4 (NOASSERTION)

Inventory item Vulnerabilities Files Audit notes Licenses Copyrights

> Filter

Resolved	ID	Aliases	Severity	Exploitability	Risk score
☒	VCD-3qjnyh1ght	CVE-2025-48924, GHSA-288-qh7-25v		0.5	3.1

Update vulnerabilities Create VEX

Item Files

Vulnerable X

archive-commons-lang3-9e7d3023abf434d23.4
archive-guava-9f5a1f12b11aaf12a8a0f0f...
archive-jansi-da83c628f61a8f708b0f0f...
archive-junit4-4c5d5b5a2778db114211...
archive-logback-core-1754e7c24315ec2911...
archive-maven-compat-05e4f16d332708da...
archive-maven-core-0f86236f35862208K...



4.17.2.3 Eclipse Mosquitto

<https://github.com/eclipse/mosquitto>

The screenshot shows the Occtet Curator interface for the 'eclipse-mosquitto-test' project. The left sidebar contains navigation links for Dashboard, SBOM Mgmt, Vulnerabilities, VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and Administration. The main area is titled 'SBOM Mgmt' and shows the 'Overview' section. The 'Files' list on the left includes a search bar and a list of files categorized by '1.2.0-0' and 'c'. The 'Overview' section on the right shows 0 Copyrights, 14 Licenses, and 0 Vulnerabilities. The 'Licenses' section is expanded, showing a list of licenses and the number of software components they apply to.

License	Number in software components
MIT	9
Apache-2.0	3
BSD-3-Clause	3
BSD-2-Clause	1
GPL-2.0-only	8
CC0-1.0	1
Zlib	1
LOPL-3.0-or-later	4

The screenshot shows the Occtet Curator interface for the 'eclipse-mosquitto-test' project. The left sidebar contains navigation links for Dashboard, SBOM Mgmt, Vulnerabilities, VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and Administration. The main area is titled 'SBOM Mgmt' and shows the 'Overview' section. The 'Files' list on the left includes a search bar and a list of files categorized by '1.2.0-0' and 'c'. The 'Overview' section on the right shows 0 Copyrights, 14 Licenses, and 0 Vulnerabilities. The 'Licenses' section is expanded, showing a list of licenses and the number of software components they apply to.

License	Number in software components
MIT	9
Apache-2.0	3
BSD-3-Clause	3
BSD-2-Clause	1
GPL-2.0-only	8
CC0-1.0	1
Zlib	1
LOPL-3.0-or-later	4



https://occtet.bitsea.de/boc/vulnerabilities

Octet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities**
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration

Vulnerabilities

Choose project
eclipse-mosquitto - test [Show all](#)

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Last update
----	---------	----------	----------------	------------	------------	-------------

[admin] [Edit](#) [Remove](#) [Excel](#) [JSON](#)

https://occtet.bitsea.de/boc/software-components

Octet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities
- VEX listing
- Projects
- Software components**
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration

Software components

Choose project
eclipse-mosquitto - test [Show all](#)

> Filter

Name	Version	PURL	Licenses	Curated	License controlled by AI
alpine-base-layout	3.7.1-r8	pkg:apk/alpine/alpine-base-layout@3.7.1-r8?arch=x86_64	GPL-2.0-only	False	
alpine-base-layout-data	3.7.1-r8	pkg:apk/alpine/alpine-base-layout-data@3.7.1-r8?arch=x86_64	GPL-2.0-only	False	
alpine-keys	2.6-r0	pkg:apk/alpine/alpine-keys@2.6-r0?arch=x86_64&distro=alpine	MIT	False	
alpine-release	3.23.3-r0	pkg:apk/alpine/alpine-release@3.23.3-r0?arch=x86_64	MIT	False	
apk-tools	3.0.3-r1	pkg:apk/alpine/apk-tools@3.0.3-r1?arch=x86_64&distro=alpine	GPL-2.0-only	False	
argon2-libs	20190702-r5	pkg:apk/alpine/argon2-libs@20190702-r5?arch=x86_64	Apache-2.0, CC0-1.0	False	
bretyl-libs	1.2.0-r0	pkg:apk/alpine/bretyl-libs@1.2.0-r0?arch=x86_64&distro=alpine	MIT	False	
busybox	1.37.0-r30	pkg:apk/alpine/busybox@1.37.0-r30?arch=x86_64&distro=alpine	GPL-2.0-only	False	
busybox-binsh	1.37.0-r30	pkg:apk/alpine/busybox-binsh@1.37.0-r30?arch=x86_64	GPL-2.0-only	False	
ca-certificates	20251003-r0	pkg:apk/alpine/ca-certificates@20251003-r0?arch=x86_64	MIT, MPL-2.0	False	True
ca-certificates-bundle	20251003-r0	pkg:apk/alpine/ca-certificates-bundle@20251003-r0?arch=x86_64	MPL-2.0, MIT	False	True
cjson	1.7.19-r1	pkg:apk/alpine/cjson@1.7.19-r1?arch=x86_64&distro=alpine	MIT	False	
gmp	6.3.0-r4	pkg:apk/alpine/gmp@6.3.0-r4?arch=x86_64&distro=alpine	LGPL-3.0-or-later, GPL-2.0-or-later	False	
gnutls	3.8.11-r0	pkg:apk/alpine/gnutls@3.8.11-r0?arch=x86_64&distro=alpine	LGPL-3.0-or-later	False	
libapk	3.0.3-r1	pkg:apk/alpine/libapk@3.0.3-r1?arch=x86_64&distro=alpine	GPL-2.0-only	False	
libcrypto3	3.5.5-r0	pkg:apk/alpine/libcrypto3@3.5.5-r0?arch=x86_64&distro=alpine	Apache-2.0	False	
libedit	20251016.3.1-r0	pkg:apk/alpine/libedit@20251016.3.1-r0?arch=x86_64	BSD-3-Clause	False	
libffi	3.5.2-r0	pkg:apk/alpine/libffi@3.5.2-r0?arch=x86_64&distro=alpine	MIT	False	
libidn2	2.3.8-r0	pkg:apk/alpine/libidn2@2.3.8-r0?arch=x86_64&distro=alpine	GPL-2.0-or-later, LGPL-3.0-or-later	False	
libmccomp	1.0.2-r1	pkg:apk/alpine/libmccomp@1.0.2-r1?arch=x86_64&distro=alpine	LGPL-2.1-or-later	False	
libncursesw	6.5_p20251123-r0	pkg:apk/alpine/libncursesw@6.5_p20251123-r0?arch=x86_64	X11	False	
libssl3	3.5.5-r0	pkg:apk/alpine/libssl3@3.5.5-r0?arch=x86_64&distro=alpine	Apache-2.0	False	

[admin] [Create](#) [Edit](#) [Remove](#)

4.17.2.4 Tomcat

<https://github.com/apache/tomcat>

The screenshot shows the Occtet Curator SBOM Mgmt interface. The left sidebar contains navigation links: Dashboard, SBOM Mgmt (selected), Vulnerabilities, VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and Administration. The main content area is titled 'Overview' and shows a list of 153 Copyrights and 24 Licenses. The 'Files' section on the right lists various files with their counts.

Copyright name	Number in files
Copyright (c) 1989, 1991 Free Software Foundation, Inc. copyrighted by the Free Software Fo...	3
Copyright 1999-@YEAR@ The Apache Software Foundation	2
Copyright 2003-2009 Sun Microsystems, Inc.	5
Copyright (c) 1999-@YEAR@ The Apache Software Foundation ViaVersionKey FileDescript...	1
Copyright (c) 1999-@YEAR@ The Apache Software Foundation	1
Copyright (c) 2000, 2004 Oracle and/or its affiliates	6
Copyright (c) 2009-2017 Oracle and/or its affiliates	4
Copyright (c) 2009, 2020 Oracle and/or its affiliates	10
Copyright 1999-2025 The Apache Software Foundation Copyright 2002-2018 Red Hat Inc. Co...	1
Copyright (c) 1999-@YEAR@ The Apache Software Foundation	1
Copyright (c) 2009-2010 Oracle and/or its affiliates	5
Copyright (c) 2000, 2021 Oracle and/or its affiliates	14
Copyright & 169 2000-@YEAR@ The Apache Software Foundation	1
(c) Copyright International Business Machines Corporation 2002	2

Item	Files #
com.fasterxml.woodstox.woodstox-core-7.1.0-sou...	79
com.fasterxml.woodstox.woodstox-core-7.1.0-vcs...	0
com.h2database.h2-2.2.220-source-artifact (LGPL...	771
com.h2database.h2-2.2.220-vcs (LGPL-2.0-or-late...	0
com.sun.istack-istack-commons-runtime-4.1.2-sou...	22
com.sun.istack-istack-commons-runtime-4.1.2-vcs...	0
jakarta.activation-jakarta.activation-api-2.1.3-sour...	34
jakarta.activation-jakarta.activation-api-2.1.3-vcs...	0
jakarta.annotation-jakarta.annotation-api-2.1.0-sou...	22
jakarta.annotation-jakarta.annotation-api-2.1.0-vcs...	0
jakarta.annotation-jakarta.annotation-api-2.1.1-sou...	22
jakarta.annotation-jakarta.annotation-api-2.1.1-vcs...	0
jakarta.annotation-jakarta.annotation-api-2.1.1-sou...	22
jakarta.annotation-jakarta.annotation-api-2.1.1-vcs...	0
jakarta.el-jakarta.el-api-5.0.0-source-artifact (EPL...	43
jakarta.el-jakarta.el-api-5.0.0-vcs (EPL-2.0-AND...	0
jakarta.enterprise-jakarta.enterprise-cdi-api-4.0.1-s...	174
jakarta.enterprise-jakarta.enterprise-cdi-api-4.0.1-v...	0
jakarta.enterprise-jakarta.enterprise-lang-model-4...	3
jakarta.enterprise-jakarta.enterprise-lang-model-4...	0
jakarta.inject-jakarta.inject-api-2.0.1-source-artifac...	10
jakarta.inject-jakarta.inject-api-2.0.1-vcs (BSD-3-C...	0
jakarta.interceptor-jakarta.interceptor-api-2.1.0-sou...	14
jakarta.interceptor-jakarta.interceptor-api-2.1.0-vcs...	0
jakarta.json-bind-jakarta.json-bind-api-3.0.1-sourc...	38
jakarta.json-bind-jakarta.json-bind-api-3.0.1-vcs (...	0
jakarta.json-jakarta.json-api-2.1.3-source-artifact (...)	39
jakarta.json-jakarta.json-api-2.1.3-vcs (BSD-3-Cla...	0
jakarta.ws.rs-jakarta.ws.rs-api-3.1.0-source-artifac...	133
jakarta.ws.rs-jakarta.ws.rs-api-3.1.0-vcs (Apache-2...	0
jakarta.xml.bind-jakarta.xml.bind-api-4.0.2-source...	106

The screenshot shows the Occtet Curator Vulnerabilities interface. The left sidebar contains navigation links: Dashboard, SBOM Mgmt, Vulnerabilities (selected), VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and Administration. The main content area is titled 'Vulnerabilities' and shows a table of vulnerabilities for the project 'tomcat - test'.

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Last update
VCD-adtp-9d6d-zua1	CVE-2024-4539, GHSA-5239-wwm-4pmq	4.3	0.5	2.1	http://public.vulnerablecode.io/vulnerabilities/VCD-adtp-9d6d-zua1	03/30/2024 13:52:17:122



https://occtet.bitsea.de/doc/software-components

Occet Curator

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT Issues
ORT Violation
Import
Help
Administration

Software components

Choose project
tomcat - test Show all

> Filter

Name	Version	PURL	Licenses	Curated	License controlled by AI
tomcat-csf	4.1.1		Zlib, CDDL-1.0, Apache-2.0, CPL-1.0, bzip2-1.0.6, EPL-1.0	False	
tomcat-jdbc	1.1.0-SNAPSHOT		Apache-2.0	False	
tomcat-owb	4.0.3		CDDL-1.0, CPL-1.0, Apache-2.0, EPL-2.0, Zlib, bzip2-1.0.6	False	
tomcat-stuffed	1.0		CDDL-1.0, CPL-1.0, Apache-2.0, EPL-2.0, Zlib, bzip2-1.0.6	False	
tomcat	db0c0aa909f2b472093291b5c196c4f389fe		EPL-2.0, CDDL-1.0, CDDL-1.0, LicenseRef-scancode-misc	False	
woodstox-core	7.1.0	pkg:maven/com.fasterxml.woodstox/woodstox-core@7.1.0	Apache-2.0	False	
h2	2.2.220	pkg:maven/com.h2database/h2@2.2.220	LGPL-2.0-or-later, BSD-3-Clause, MPL-2.0, Unknown, L	False	
istack-commons-runtime	4.1.2	pkg:maven/com.sun.istack/istack-commons-runtime@4.1.2	BSD-3-Clause	False	
jakarta.activation-api	2.1.3	pkg:maven/jakarta.activation/jakarta.activation-api@2.1.3	Apache-2.0, GPL-2.0-only, BSD-3-Clause, EPL-2.0	False	
jakarta.annotation-api	2.1.0	pkg:maven/jakarta.annotation/jakarta.annotation-api@2.1.0	GPL-2.0-only, CDDL-1.0	False	
jakarta.annotation-api	2.1.1	pkg:maven/jakarta.annotation/jakarta.annotation-api@2.1.1	EPL-2.0, CDDL-1.0, GPL-2.0-only	False	
jakarta-el-api	5.0.0	pkg:maven/jakarta.el/jakarta-el-api@5.0.0	GPL-2.0-only, EPL-2.0, Unknown	False	
jakarta.enterprise-cdi-api	4.0.1	pkg:maven/jakarta.enterprise/jakarta.enterprise-cdi-api@4.0.1	Apache-2.0, Unknown, EPL-2.0	False	
jakarta.enterprise-lang-model	4.0.1	pkg:maven/jakarta.enterprise/jakarta.enterprise-lang-model@4.0.1	Apache-2.0, EPL-2.0, Unknown	False	
jakarta.inject-api	2.0.1	pkg:maven/jakarta.inject/jakarta.inject-api@2.0.1	BSD-3-Clause, Apache-2.0	False	
jakarta.json.bind-api	3.0.1	pkg:maven/jakarta.json.bind/jakarta.json.bind-api@3.0.1	GPL-2.0-only, EPL-2.0	False	
jakarta.ws.rs-api	3.1.0	pkg:maven/jakarta.ws.rs/jakarta.ws.rs-api@3.1.0	CPL-1.0, EPL-2.0, Apache-2.0, GPL-2.0-only, EPL-1.0	False	
jakarta.xml.bind-api	4.0.2	pkg:maven/jakarta.xml.bind/jakarta.xml.bind-api@4.0.2	BSD-3-Clause, Unknown	False	
junix	4.13.2	pkg:maven/junix/junix@4.13.2	EPL-1.0	False	
csf-core	4.1.1	pkg:maven/org.apache.csf/csf-core@4.1.1	Apache-2.0	False	
csf-integration-cdi	4.1.1	pkg:maven/org.apache.csf/csf-integration-cdi@4.1.1	Apache-2.0	False	
csf-rs-client	4.1.1	pkg:maven/org.apache.csf/csf-rs-client@4.1.1	Apache-2.0	False	

[admin] Create Edit Remove

4.17.2.5 Kafka

<https://github.com/apache/kafka>

vulnerabilities:8

Occet Curator

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT Issues
ORT Violation
Import
Help
Administration

SBOM Mgmt

Choose project
Kafka - 4.2.0

Search files... Show all

Files
> dependencies

Overview **Inventory items**

bcrypt-5.0.0-source-artifact (Apache-2.0) com.fasterxml.jackson.core-jackson-core-2.19.2-source-artifact (Apache-2.0)

Inventory Item **Vulnerabilities** Files Audit notes Licenses Copyrights

> Filter

Resolved	ID	Aliases	Severity	Exploitability	Risk score
1	VGD-q868-Map-hyc7	GHS472hv-8253-57q	Medium	0.5	4

Update vulnerabilities Create VEX

Vulnerability

Item	Files
com.fasterxml.jackson.core-jackson-core-2.19.2	0
com.fasterxml.jackson.core-jackson-core-2.19.2	28
com.fasterxml.jackson.core-jackson-core-2.19.2	0
jms-2.0.3-source-artifact (BSD-3-Clause)	0
jms-2.0.3-vcs (BSD-3-Clause)	5
paramiko-2.10.6 ((LGPL-2.0-or-later AND L...))	0
paramiko-2.10.6-source-artifact ((LGPL-2.0...))	0
paramiko-2.10.6-vcs ((LGPL-2.0-or-later AN...))	71
pcrcrypto-2.6.1-source-artifact (LicenseRef-...)	0
pcrcryptodome-3.9.8 ((LicenseRef-scancode...))	170
pcrcryptodome-3.9.8-source-artifact ((Licen...))	259
pyyaml-5.3.1 (MIT)	0
pyyaml-5.3.1-source-artifact (MIT)	0
pyyaml-5.3.1-vcs (MIT)	5
requesto-2.31.0 (Apache-2.0)	0
requesto-2.31.0-source-artifact (Apache-2.0)	0
requesto-2.31.0-vcs (Apache-2.0)	13
urllib3-1.26.20-source-artifact (MIT)	0
urllib3-1.26.20-vcs (MIT)	11
zoo-1.2.0 (MIT)	0
zoo-1.2.0-source-artifact (MIT)	0
zoo-1.2.0-vcs (MIT)	2



SBOM Mgmt

Choose project: **Kafka - 4.2.0**

Search files... **Show all**

Files: **dependencies**

VEX data

Timestamp: 04/23/2026 11:55:30:760

Title:

BOM format: Spec version: Serial number: Version:

BOM format required: Spec version required: Serial number required: Version required:

Metadata

Type:

Component version:

Component name:

Save & download **Close**

Vulnerabilities

Choose project: **Kafka - 4.2.0**

Filter

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
VDD-q6k8-l4p-hy7	GHS-72h-8235-57q	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDD-q6k8-l4p-hy7	False	04/07/2026 09:57:56:675
VDD-refe-65b-87c	CVE-2025-64418, GHSA-gm62-cv2-4w53	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDD-refe-65b-87c	False	04/13/2026 12:35:06:278
VDD-swpv-7yhh-x3ev	CVE-2025-21441, GHSA-8b9y-5279-wg99	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDD-swpv-7yhh-x3ev	False	04/13/2026 12:35:06:278
VDD-y8k6-cz51-c5ee	CVE-2025-64471, GHSA-2zpw-wfqp-9737	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDD-y8k6-cz51-c5ee	False	04/13/2026 12:35:06:278
VDD-b67h-2au2-aaam	CVE-2024-5565, GHSA-fm9-94q-7637	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDD-b67h-2au2-aaam	False	04/17/2026 14:26:35:258
VDD-58m1-m13v-aaae	CVE-2024-22195, GHSA-l8c8-rqap-cp95	Low	0.5	3.6	http://public.vulnerablecode.io/vulnerabilities/VDD-58m1-m13v-aaae	False	04/23/2026 11:51:09:347
VDD-b7hu-w9d8-w7ga	CVE-2024-56201, GHSA-gm9f-6f8f-6699	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDD-b7hu-w9d8-w7ga	False	04/23/2026 11:51:09:450
VDD-c5f6-cf9q-aaqj	CVE-2024-34064, GHSA-a75v-3vq-5m5j	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDD-c5f6-cf9q-aaqj	False	04/23/2026 11:51:09:450
VDD-s5g7-avsk-plfv	CVE-2024-56326, GHSA-q2a7-8v6-6q7h	Low	0.5	3.5	http://public.vulnerablecode.io/vulnerabilities/VDD-s5g7-avsk-plfv	False	04/23/2026 11:51:09:609
VDD-dhvd-jl8z-vqbh	CVE-2025-27516, GHSA-cpww-rp4-4qg7	Low	0.5	3.3	http://public.vulnerablecode.io/vulnerabilities/VDD-dhvd-jl8z-vqbh	False	04/23/2026 11:51:09:651
VDD-suan-53ay-aaaa	CVE-2023-48795, GHSA-49a7-px36-v8w8	Critical	2	10	http://public.vulnerablecode.io/vulnerabilities/VDD-suan-53ay-aaaa	False	04/23/2026 11:51:13:406
VDD-4gjd-vh3-aaad	CVE-2018-4594, GHSA-6528-wr6-66q, PYSEC-2018-97	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDD-4gjd-vh3-aaad	False	04/23/2026 11:51:16:150
VDD-l2k4-fgk-aaaa	CVE-2013-7459, GHSA-cq27-w7p-c356, PYSEC-2017-54	Medium	0.5	4.5	http://public.vulnerablecode.io/vulnerabilities/VDD-l2k4-fgk-aaaa	False	04/23/2026 11:51:16:202
VDD-pq9f-spg8-aaab	CVE-2023-52323, GHSA-q225-cvav-gx7, PYSEC-2024-3	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDD-pq9f-spg8-aaab	False	04/23/2026 11:51:16:759
VDD-qnc3-8m8-aaah	CVE-2020-14343, GHSA-8q59-qd8h-6h4, PYSEC-2021-142	Medium	0.5	4.5	http://public.vulnerablecode.io/vulnerabilities/VDD-qnc3-8m8-aaah	False	04/23/2026 11:51:20:125
VDD-gkuw-ese7-4b67	CVE-2024-47081, GHSA-8w4-k78v-vn56	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDD-gkuw-ese7-4b67	False	04/23/2026 11:51:22:041
VDD-wsth-kwqz-aaak	CVE-2024-35195, GHSA-pq67-6m6q-mj2v	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDD-wsth-kwqz-aaak	False	04/23/2026 11:51:22:121
VDD-l8ap-4gpc-1qf1	CVE-2025-9181, GHSA-pq67-6m6q-mj2v	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDD-l8ap-4gpc-1qf1	False	04/23/2026 11:51:26:506

Create **Edit** **Remove** **Excel** **JSON**



4.17.3 Python projects

4.17.3.1 Type-extensions 4.13.2

https://github.com/python/typing_extensions

The screenshot shows the Occtet Curator SBOM Mgmt interface. The left sidebar contains navigation links: Dashboard, SBOM Mgmt, Vulnerabilities, VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and Administration. The main content area is titled 'SBOM Mgmt' and shows the 'Overview' tab for the project 'type-extensions - 4.13.2'. The Overview tab displays sections for Copyrights (0), Licenses (0), and Vulnerabilities (0). On the right, there is a 'Files' section with a table listing files and their hashes. The table has columns for 'Item' and 'Files #'. The files listed are: typingextensions-main-d04748 (NOA...), checkout-6-75c4466-75c4466 (NOA...), codecov-action-671740ac38099..., download-artifact-8-75c4466-75c4466 (NOA...), gh-action-pypi-publish-e0c6393..., github-script-8-75c4466-75c4466 (NOA...), setup-python-6-75c4466-75c4466 (NOA...), sh-setup-uv-1e862f6c0d105e8..., and upload-artifact-7-75c4466-75c4466 (NOA...). Each file has a status indicator (green circle with a checkmark or red circle with an exclamation mark).

The screenshot shows the Occtet Curator Vulnerabilities interface. The left sidebar contains navigation links: Dashboard, SBOM Mgmt, Vulnerabilities, VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and Administration. The main content area is titled 'Vulnerabilities' and shows the 'type-extensions - 4.13.2' project. The interface displays a table with columns: ID, Aliases, Severity, Exploitability, Risk score, Source URL, Manually created, and Last update. The table is currently empty. At the bottom, there are buttons for '+ Create', 'Edit', and 'Remove'. On the right, there are buttons for 'Excel' and 'JSON'.

4.17.3.2 idna -3.10.0
<https://github.com/kjd/idna>

OCCTET Deliverable Number: D 3.3 - SME Toolkit-Demo-Del - page 86



https://occtet.bitsea.de/boc/vulnerabilities

Octet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities**
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ! ORT Issues
- ! ORT Violation
- Import
- Help
- Administration

Vulnerabilities

Choose project
idna - 3.10.0

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

[curator-admin] [+ Create](#) [Edit](#) [Remove](#) [Excel](#) [JSON](#)

https://occtet.bitsea.de/boc/software-components

Octet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities
- VEX listing
- Projects
- Software components**
- Inventory
- Licenses
- Copyrights
- ! ORT Issues
- ! ORT Violation
- Import
- Help
- Administration

Software components

Choose project
idna - 3.10.0

> Filter

11 rows

Name	Version	PURL	Licenses	Curated	License controlled by AI
actions/setup-python	a26af9be951a213d495a6c3e4e4022e16d877085	pkg:githubactions/actions/setup-python@a26af9be9...		False	
actions/download-artifact	d3f88a106a0bac45b9774a628896c90bd0f5c8093	pkg:githubactions/actions/download-artifact@d3f88a...		False	
sigstore/gh-action-sigstore-python	f514646997ebcd3bdc05145c30b9c1edd0b46	pkg:githubactions/sigstore/gh-action-sigstore-python...		False	
actions/checkout	110d719010be5b1630ceea73d77597364c4af9683	pkg:githubactions/actions/checkout@110d719010be5...		False	
pyppa/gh-action-pypi-publish	7d052bc84231f629af0346d9f1284150baab0fc	pkg:githubactions/pyppa/gh-action-pypi-publish@7d052...		False	
actions/upload-artifact	ea1659b0556a675b540449f2d48886430679a02	pkg:githubactions/actions/upload-artifact@ea1659b05...		False	
github/codeql-action/upload-sarif	17573ee1cc109d061760f3a0066c4aac49f448c5	pkg:githubactions/github/codeql-action/upload-sarif@...		False	
actions/checkout	692973e3d9371299c9f40652e90291b0c73332	pkg:githubactions/actions/checkout@692973e3d9371...		False	
ossf/scorecard-action	a46b90b4cac8162298cc4d9bdc90d3dfe707096	pkg:githubactions/ossf/scorecard-action@a46b90b4c...		False	
actions/upload-artifact	8341144e995460balle113a2bc961336a5ec5a	pkg:githubactions/actions/upload-artifact@8341144e...		False	
com.github.kjd/idna	master	pkg:github/kjd/idna@master	BSD-3-Clause	False	

[curator-admin] [+ Create](#) [Edit](#) [Remove](#)



4.17.3.3 Certifi 2025.4.26



Octet Curator
Software components

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

[Choose project](#)

Certifi - 2025.4.6

> Filter

Name ▾	Version ▾	PURL ▾	Licenses ▾	Curated ▾	License controlled by AI ▾
actions/checkout	defac2e4500abe009fe7214ff5f447c683de	pkg:github.com/actions/checkout@defac2e4500d...		False	
peter-evans/create-pull-request	56978fa089642200dc7764989d070b2cc71	pkg:github.com/peter-evans/create-pull-request@5f...		False	
actions/setup-python	a309f8ba42658ecde2a45f086646889bd2405	pkg:github.com/actions/setup-python@a309f8ba42...		False	
dessant/lock-threads	726ea7cxc5cd8fb1c6db358fc08fc7376adbe7	pkg:github.com/dessant/lock-threads@726ea7cxc...		False	
psypa/gh-action-yppi-publish	cfe221992ed1bac3cc03623a2687e10172e277b	pkg:github.com/psypa/gh-action-yppi-publish@cfe22...		False	
actions/download-artifact	3e54562cb9f17205464087a4be9de05a5481e7c	pkg:github.com/actions/download-artifact@3e545...		False	
actions/upload-artifact	0439a46d1a93c77aa656e7c1c64a87561c5da8	pkg:github.com/actions/upload-artifact@0439a46d1...		False	
com.github.cerifi/python-certifi	master	pkg:github.com/cerifi/python-certifi@master		False	

+ Create

Edit

Remove

4.17.3.4 Six-1.17.0

<https://github.com/benjaminp/six>

https://occtet.bitsea.de/boc/audit-view/502

Occtet Curator

SBOM Mgmt

Choose project

Six - 1.17.0

Search files...

Show all

Files

Overview

> Copyrights (0)

< Licenses (1)

License	Number in software components
MIT	1

> Vulnerabilities (0)

Item

Files #

six-main-432b53 (MIT)	0
75c946 (NOASSERTION)	0
checkio-5_75c9465.* (NOAS...	0
setup-python-6_75c9466.* (N...	0

[curator-admin]



https://occtet.bitsea.de/boc/vulnerabilities

Occtet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities**
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration

Vulnerabilities

Choose project
Six - 1.17.0

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

[curator-admin] [+ Create](#) [Edit](#) [Remove](#) [Excel](#) [JSON](#)

https://occtet.bitsea.de/boc/software-components

Occtet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities
- VEX listing
- Projects
- Software components**
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration

Software components

Choose project
Six - 1.17.0

> Filter 4 rows

Name	Version	PURL	Licenses	Curated	License controlled by AI
pytest		pkg:pytest/pytest		False	
actions/setup-python	6.**	pkg:githubactions/actions/setup-python@6.%2A.%2A		False	
com.github.benjaminc/six	main	pkg:github.com/benjaminc/six/main	MIT	False	
actions/checkout	5.**	pkg:githubactions/actions/checkout@5.%2A.%2A		False	

[curator-admin] [+ Create](#) [Edit](#) [Remove](#)



4.17.3.5 Charset-normalizer-3.4.1

https://github.com/jawah/charset_normalizer

Vulnerabilities: 4

Octet Curator | SBOM Mgmt | Choose project: **charset-normalizer - 3.4.1**

Overview

- > Copyrights (5)
- > Licenses (11)
- > Vulnerabilities (4)

Vulnerability	Risk score of vulnerability	Number in software components
VDB-2025-22701	3.1	3
VDB-2025-22701	3.1	1
VDB-2025-22701	3.1	3
VDB-2025-22701	3.1	1

Files

- charsetnormalizer-master-62111...
- 0.4.0-75c946 (IPSF-2.0 AND ...)
- 0.4.6-75c946 (BSD-3-Clause ...)
- 1.1.1-75c946 (MIT)
- 1.2.0-75c946 (MIT)
- 1.2.2-post1-75c946 (MIT)
- 1.3.1-75c946 (MIT AND PyD...
- 1.4.0-75c946 (NOASSERTION)
- 1.5.0-75c946 (MIT)
- 1.6.0-75c946 (MIT)
- 2.0.0-75c946 (MIT)
- 2.0.1-75c946 (MIT)
- 2024.4.15-75c946 (Apache 2...
- 2025.2.9-75c946 (NOASSERT...
- 20.26.6-75c946 (MIT)
- 2.1.0-75c946 (MIT)
- 21.2.0-75c946 (MIT)
- 2.20.0-75c946 (BSD-2-Clause)
- 2.3.0-75c946 (MIT)
- 24.0-75c946 (BSD-2-Clause ...)
- 2.4.1-75c946 (MIT)
- 25.0.0-75c946 (MIT)
- 26.0-75c946 (BSD-2-Clause ...)
- 26.1.0-75c946 (MIT)
- 3.12.2-75c946 (Unlicense)
- 3.1.2-75c946 (Apache 2.0)
- 3.15.0-75c946 (MIT)
- 3.16.1-75c946 (Unlicense)
- 3.19.1-75c946 (Unlicense)

Octet Curator | SBOM Mgmt | Choose project: **charset-normalizer - 3.4.1**

Vulnerabilities

3.12.2-75c946 (Unlicense) x 20.26.6-75c946 (MIT) x 3.15.0-75c946 (MIT) x

Inventory item | Vulnerabilities | Files | Audit notes | Licenses | Copyrights

Filter | 2 rows

Resolved	ID	Aliases	Severity	Exploitability	Risk score
☐	VDB-2025-22701	CVE-2025-22701, GHSA-qmhc-5htg-mrnx	Low	0.5	3.1
☐	VDB-2025-22701	CVE-2025-22701, GHSA-qmhc-5htg-mrnx	Low	0.5	3.1

[Update vulnerabilities](#) [Create VEX](#)

Files

- 20.26.6-75c946 (MIT)
- 3.12.2-75c946 (Unlicense)
- 3.15.0-75c946 (MIT)
- 3.16.1-75c946 (Unlicense)
- 3.19.1-75c946 (Unlicense)



OCCTET Curator Dashboard SBOM Mgmt Vulnerabilities VEX listing Projects Software components Inventory Licenses Copyrights ORT Issues ORT Violation Import Help Administration	Vulnerabilities									
	Choose project									
	charset-normalizer - 3.0.0									
	> Filter									

OCCTET Curator Dashboard SBOM Mgmt Vulnerabilities VEX listing Projects Software components Inventory Licenses Copyrights ORT Issues ORT Violation Import Help Administration	Software components									
	Choose project									
	charset-normalizer - 3.0.0									
	> Filter									



4.17.3.6 Requests-2.32.3

<https://github.com/psf/requests>

Vulnerabilities: 4

Overview

> Copyrights (0)

> Licenses (4)

> Vulnerabilities (4)

Vulnerability	Risk score of vulnerability	Number in software components
VCD-3ao-usaz-aag	3.4	1
VCD-496-vggm-aac	3.1	1
VCD-12z1-d3ag-aag	4.4	1
VCD-mg48-8meh-aaa	4	1

Items

requests-main-df5a21 (Apache 2.0)

7.2.6-75c44 (BSD-3-Clause ANL)

75c44-- 6.10.0 (NOASSERTION)

75c44-- 1.26. 3 (NOASSERTION)

75c44-- 2023.5.7 (NOASSERTION)

75c44-- 2.3. 4 (NOASSERTION)

75c44-- 2.8.0. 10 (NOASSERTION)

75c44 (NOASSERTION)

action-analyze-c10b804de649...

action-autobuild-c10b804de649...

action-mix-c10b804de6491lea...

checkout-def0a2e4300abe0...

commit-action-646c33c0d4002...

cov-75c44 (NOASSERTION)

download-artifact-70c10c65e...

gh-action-pypi-publish-ed0c3393...

httpbin-2.1.0-75c44 (MIT)

lock-threads-7264a7c5c1d910...

normalizer-75c44-- 2. 4 (NOA...

setup-python-309f8b426d58ec...

upload-artifact-6bbca2d5aa5d8f...

zizmor action-71221a20a9ed1...

Overview

> Copyrights (0)

> Licenses (4)

> Vulnerabilities (4)

License	Number in software components
MIT	1
Apache 2.0	1
BSD-3-Clause	1
BSD-2-Clause	1

Items

requests-main-df5a21 (Apache 2.0)

7.2.6-75c44 (BSD-3-Clause ANL)

75c44-- 6.10.0 (NOASSERTION)

75c44-- 1.26. 3 (NOASSERTION)

75c44-- 2023.5.7 (NOASSERTION)

75c44-- 2.3. 4 (NOASSERTION)

75c44-- 2.8.0. 10 (NOASSERTION)

75c44 (NOASSERTION)

action-analyze-c10b804de649...

action-autobuild-c10b804de649...

action-mix-c10b804de6491lea...

checkout-def0a2e4300abe0...

commit-action-646c33c0d4002...

cov-75c44 (NOASSERTION)

download-artifact-70c10c65e...

gh-action-pypi-publish-ed0c3393...

httpbin-2.1.0-75c44 (MIT)

lock-threads-7264a7c5c1d910...

normalizer-75c44-- 2. 4 (NOA...

setup-python-309f8b426d58ec...

upload-artifact-6bbca2d5aa5d8f...

zizmor action-71221a20a9ed1...



https://occtet.bitsea.de/boc/audit-view/504

Occtet Curator

SBOM Mgmt

Choose project: requests - 2.32.3

Search files...

Show all

Files

Overview Inventory items

75c946== 1.26, < 3 (NOASSERTION) x 75c946== 2023.5.7 (NOASSERTION) x

Inventory item Vulnerabilities Files Audit notes Licenses Copyrights

Save

Filter

Resolved	ID	Aliases	Severity	Exploitability	Risk score
☐	VCD-1221-d2ag-aaag	CVE-2023-37920, GHSA-xqr8-7je-rhp, PYSEC-2023-135	Medium	0.5	4.4

Update vulnerabilities Create VEX

[curator-admin]

https://occtet.bitsea.de/boc/vulnerabilities

Occtet Curator

Vulnerabilities

Choose project: requests - 2.32.3

Filter

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
VCD-3au-usaz-aaag	CVE-2024-3651, GHSA-jig7-24vr-x38h, PYSEC-2024-40	Low	0.5	3.4	http://public.vulnerabilitycode.io/vulnerabilities/VCD-3au-usaz-aaag	False	04/16/2024 13:29:10:087
VCD-496-vgrm-aaac	CVE-2023-45803, GHSA-g4mx-qhvg-27pA, PYSEC-2023-45803, PYSEC-2023-212	Low	0.5	3.1	http://public.vulnerabilitycode.io/vulnerabilities/VCD-496-vgrm-aaac	False	04/17/2024 12:09:04:313
VCD-1221-d2ag-aaag	CVE-2023-37920, GHSA-xqr8-7je-rhp, PYSEC-2023-135	Medium	0.5	4.4	http://public.vulnerabilitycode.io/vulnerabilities/VCD-1221-d2ag-aaag	False	04/17/2024 12:09:07:876
VCD-mg48-8mnh-aaaa	CVE-2022-40898, GHSA-qwmp-3cf2-gfgh, PYSEC-2023-40898, PYSEC-2022-43017	Medium	0.5	4	http://public.vulnerabilitycode.io/vulnerabilities/VCD-mg48-8mnh-aaaa	False	04/17/2024 12:09:14:604

[curator-admin] + Create Edit Remove

Excel JSON

https://occtet.bitsea.de/boc/copyrights



OCCTET Curator

Software components

Choose project

requests - 2.32.3

Filter

Name	Version	PURL	Licenses	Curated	License controlled by AI
actions/checkout	de0fac2e4500da0e009e67214ff5f547ce83dd	pkg:githubactions/actions/checkout@de0fac2e4500...		False	
actions/setup-python	a309f8b42b58c9e2a4509869646886d02405	pkg:githubactions/actions/setup-python@a309f8b42...		False	
dessant/lock-threads	7266a7ce5c1d01b1c6db850fcd86c7375dadb7	pkg:githubactions/dessant/lock-threads@7266a7ce5c...		False	
actions/upload-artifact	bb0ca2d5aa5d8f6aa3e3b6766aad77386f024f	pkg:githubactions/actions/upload-artifact@bb0ca2d5...		False	
github/codeql-action/init	c10b004d664f91fa52454123d0e5e952f13	pkg:githubactions/github/codeql-action/init@c10b00...		False	
github/codeql-action/analyze	c10b004d664f91fa52454123d0e5e952f13	pkg:githubactions/github/codeql-action/analyze@c10...		False	
github/codeql-action/autobuild	c10b004d664f91fa52454123d0e5e952f13	pkg:githubactions/github/codeql-action/autobuild@c...		False	
pyppa/gh-action-pypi-publish	ed0c53931b1d69d32be73a98c796766f8a327e	pkg:githubactions/pyppa/gh-action-pypi-publish@ed0c...		False	
spgits	7.2.6	pkg:pyppa/spgits@7.2.6	BSD-3-Clause, BSD-2-Clause	False	
urllib3	>= 1.26, < 3	pkg:pyppa/urllib3		False	
charset-normalizer	>= 2, < 4	pkg:pyppa/charset-normalizer		False	
certifi	>= 2023.5.7	pkg:pyppa/certifi		False	
idna	>= 2.5, < 4	pkg:pyppa/idna		False	
pre-commit/action	646c330d0022954eaf5a54b4d0193ce7f9507	pkg:githubactions/pre-commit/action@646c330d00...		False	
actions/download-artifact	70610cde5e1e46a2ead62b72a43f7947b13c3	pkg:githubactions/actions/download-artifact@70610...		False	
zcmorcore/zcmor-action	71321a20a9bed102f6fcd5718a2cac2c4f70d8	pkg:githubactions/zcmorcore/zcmor-action@71321a...		False	
httpbin	>= 0.10.0	pkg:pyppa/httpbin		False	
pyrest-httpbin	2.1.0	pkg:pyppa/pyrest-httpbin@2.1.0	MIT	False	
pyrest	>= 2.8.0, < 10	pkg:pyppa/pyrest		False	
wheel		pkg:pyppa/wheel		False	
pyrest-cov		pkg:pyppa/pyrest-cov		False	
com.github.pfif.requests	main	pkg:githubpfif/requests@main	Apache 2.0	False	

+ Create Edit Remove

OCCTET Curator

Software components

Choose project

requests - 2.32.3

Filter

Refresh Add search condition

Name	Version	PURL	Licenses	Curated	License controlled by AI
actions/checkout	de0fac2e4500da0e009e67214ff5f547ce83dd	pkg:githubactions/actions/checkout@de0fac2e4500...		False	
actions/setup-python	a309f8b42b58c9e2a4509869646886d02405	pkg:githubactions/actions/setup-python@a309f8b42...		False	
dessant/lock-threads	7266a7ce5c1d01b1c6db850fcd86c7375dadb7	pkg:githubactions/dessant/lock-threads@7266a7ce5c...		False	
actions/upload-artifact	bb0ca2d5aa5d8f6aa3e3b6766aad77386f024f	pkg:githubactions/actions/upload-artifact@bb0ca2d5...		False	
github/codeql-action/init	c10b004d664f91fa52454123d0e5e952f13	pkg:githubactions/github/codeql-action/init@c10b00...		False	
github/codeql-action/analyze	c10b004d664f91fa52454123d0e5e952f13	pkg:githubactions/github/codeql-action/analyze@c10...		False	
github/codeql-action/autobuild	c10b004d664f91fa52454123d0e5e952f13	pkg:githubactions/github/codeql-action/autobuild@c...		False	
pyppa/gh-action-pypi-publish	ed0c53931b1d69d32be73a98c796766f8a327e	pkg:githubactions/pyppa/gh-action-pypi-publish@ed0c...		False	
spgits	7.2.6	pkg:pyppa/spgits@7.2.6	BSD-3-Clause, BSD-2-Clause	False	
urllib3	>= 1.26, < 3	pkg:pyppa/urllib3		False	
charset-normalizer	>= 2, < 4	pkg:pyppa/charset-normalizer		False	
certifi	>= 2023.5.7	pkg:pyppa/certifi		False	
idna	>= 2.5, < 4	pkg:pyppa/idna		False	
pre-commit/action	646c330d0022954eaf5a54b4d0193ce7f9507	pkg:githubactions/pre-commit/action@646c330d00...		False	
actions/download-artifact	70610cde5e1e46a2ead62b72a43f7947b13c3	pkg:githubactions/actions/download-artifact@70610...		False	
zcmorcore/zcmor-action	71321a20a9bed102f6fcd5718a2cac2c4f70d8	pkg:githubactions/zcmorcore/zcmor-action@71321a...		False	
httpbin	>= 0.10.0	pkg:pyppa/httpbin		False	
pyrest-httpbin	2.1.0	pkg:pyppa/pyrest-httpbin@2.1.0	MIT	False	
pyrest	>= 2.8.0, < 10	pkg:pyppa/pyrest		False	
wheel		pkg:pyppa/wheel		False	

+ Create Edit Remove



4.17.3.7 Urllib3-2.4.0

<https://github.com/urllib3/urllib3>

Vulnerabilities: 17

Occtet Curator SBOM Mgmt

Choose project: **urllib3 - 2.4.0**

Search files...

Show all

Overview

- Copyrights (168)
- Licenses (20)
- Vulnerabilities (17)

Vulnerability	Risk score of vulnerability	Number in software components
VCID-wdtp-Rdad-zua1	2.1	1
VCID-eBht-2z64-qhv	1.9	1
VCID-4tyf-6bvo-g7cx	3.1	1
VCID-73rx-jpg5-wkdu	3.1	1
VCID-5m3b-fc3h-tyfr	4	2
VCID-47fs-3zt3-pqgh	3.1	1
VCID-vbaw-7w6p-1qhm	3.1	1
VCID-1vrs-dn11-aaak	4	1
VCID-4q68-brd1-aaah	4	1

curator-admin

Occtet Curator SBOM Mgmt

Choose project: **urllib3 - 2.4.0**

Search files...

Show all

Overview

- Copyrights (168)
- Licenses (20)
- Vulnerabilities (17)

Copyright name	Number in files
Copyright (c) 1991 - 1995, Stichting Mathematisch Centrum Amsterdam, The Netherlands Copyright (...)	5
Copyright (c) 2015 Hynek Schiawack	2
(c) N Revealed	2
Copyright 2007-2019 by the Sphinx team	14
Copyright (c) 2013-2025, Kim Davies and contributors	2
Copyright (c) Donald Stufft and individual contributors	5
Copyright (c) 2017-present Olek Lev - oss@olek.dev	3
copyright 2016, Holger Korkel	2
Copyright (c) 2015 holger korkel (rather uses bitbucket/hg42)	2
Copyright (c) Curve FL 2020-2023	6
Copyright (c) 2009 Benjamin Kowarsch	6
Copyright (c) 2005-2007 Terence Parr	6
Copyright 1999-2011 (VVV)	3
Copyright (c) 2003, MetaQuotes Software Corp Copyright 2006-2014, MetaQuotes Software Corp. Int...	3

curator-admin



Octet Curator	Vulnerabilities
Dashboard	
SBOM Mgmt	
Vulnerabilities	
VEX listing	
Projects	
Software components	
Inventory	
Licenses	
Copyrights	
ORT Issues	
ORT Violation	
Import	
Help	
Administration	

Choose project

urllib - 2.4.0

> Filter

17 rows

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
VDD-ad8p-9da6-zua1	CVE-2020-4339, GHSA-3239-wwwm-4qmj	Low	0.5	2.1	http://public.vulnerablecode.io/vulnerabilities/VDD-ad8p-9da6-zua1		03/30/2020 13:52:17:122
VDD-ebf8-2zq4-1qhv	CVE-2020-27205, GHSA-68rp-wp8e-4726	Low	0.5	1.9	http://public.vulnerablecode.io/vulnerabilities/VDD-ebf8-2zq4-1qhv	False	04/16/2020 13:28:48:387
VDD-a1yf-nbvs-p7cx	CVE-2020-22701, GHSA-48rp-9d3p-mmxv	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDD-a1yf-nbvs-p7cx	False	04/16/2020 13:28:30:046
VDD-73rx-gp05-wkdu	CVE-2020-22702, GHSA-597p-3p0w-6986	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDD-73rx-gp05-wkdu	False	04/16/2020 13:28:51:036
VDD-5m3b-6d5b-fydr	CVE-2020-26007, GHSA-r6pb-v2qm-q3c2	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDD-5m3b-6d5b-fydr	False	04/16/2020 13:28:52:166
VDD-07fs-3zr3-pghm	CVE-2020-27199, GHSA-2hqc-49wr-vmda	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDD-07fs-3zr3-pghm	False	04/16/2020 13:29:01:044
VDD-vbaw-7wlp-1ghm	CVE-2020-21860, GHSA-87hc-h4s5-73r7	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDD-vbaw-7wlp-1ghm	False	04/16/2020 13:29:01:144
VDD-1vrs-dt11-aaak	CVE-2020-25659, GHSA-hggm-pg3j-v476, PYSEC-2021-62	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDD-1vrs-dt11-aaak	False	04/16/2020 13:29:02:217
VDD-4p68-brt1-aaah	GHSA-5cpq-8w7-nf7x, OMS-2023-1778	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDD-4p68-brt1-aaah	False	04/16/2020 13:29:02:299
VDD-9wts-9dbn-aaam	CVE-2023-0286, GHSA-47p-2hf-3mr5	Critical	2	10	http://public.vulnerablecode.io/vulnerabilities/VDD-9wts-9dbn-aaam	False	04/16/2020 13:29:02:430
VDD-dthe-4c49-aaan	CVE-2023-50782, GHSA-3w4d-gq4f-p7f7	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDD-dthe-4c49-aaan	False	04/16/2020 13:29:02:505
VDD-d7fk-xemc-aaar	CVE-2023-38325, GHSA-c7fp-pm7m-833m, PYSEC-2023-112	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDD-d7fk-xemc-aaar	False	04/16/2020 13:29:02:576
VDD-j6cb-jm4-aaas	GHSA-32q3-p9w5-fwm7, PYSEC-2021-63	Medium	0.5	4.5	http://public.vulnerablecode.io/vulnerabilities/VDD-j6cb-jm4-aaas	False	04/16/2020 13:29:02:639
VDD-jm31-c3d3-aaap	CVE-2024-0727, GHSA-9v8h-cq8-864p	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDD-jm31-c3d3-aaap	False	04/16/2020 13:29:02:706
VDD-vqz2-zofq-aaab	CVE-2023-23931, GHSA-w7pp-m8wf-y6f6, PYSEC-0000-CVE-2023-23931, PYSEC-2023-11	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDD-vqz2-zofq-aaab	False	04/16/2020 13:29:02:773
VDD-w668-5d2g-aaar	GHSA-jm77-qh8f-c4w8, OMS-2023-1898	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDD-w668-5d2g-aaar	False	04/16/2020 13:29:02:837
VDD-3jau-usaz-aaag	CVE-2024-3651, GHSA-j8p7-2v4v-x38h, PYSEC-2024-60	Low	0.5	3.4	http://public.vulnerablecode.io/vulnerabilities/VDD-3jau-usaz-aaag	False	04/16/2020 13:29:10:087

[curator-admin]

+ Create Edit Remove

Excel JSON

Octet Curator	Software components
Dashboard	
SBOM Mgmt	
Vulnerabilities	
VEX listing	
Projects	
Software components	
Inventory	
Licenses	
Copyrights	
ORT Issues	
ORT Violation	
Import	
Help	
Administration	

Choose project

urllib - 2.4.0

> Filter

1-100 rows of

Name	Version	PURL	Licenses	Curated	License controlled by AI
babel	2.17.0	pkg:pypi/babel@2.17.0	Unknown, BSD-3 Clause, BSD-2 Clause, LicenseRef-sc...	False	
beautifulsoup4	4.14.2	pkg:pypi/beautifulsoup4@4.14.2	Unknown, MIT, GPL-1.0-or-later	False	
certifi	2025.10.5	pkg:pypi/certifi@2025.10.5	MPL-2.0, Unknown	False	
imageio	1.4.1	pkg:pypi/imageio@1.4.1	Unknown, MIT	False	
jinja2	3.1.6	pkg:pypi/jinja2@3.1.6	BSD-3 Clause, BSD-2 Clause	False	
markupsafe	3.0.3	pkg:pypi/markupsafe@3.0.3	BSD-3 Clause	False	
mdit-py-plugins	0.5.0	pkg:pypi/mdit-py-plugins@0.5.0	Unknown, MIT	False	
mdurl	0.1.2	pkg:pypi/mdurl@0.1.2	MIT	False	
packaging	25.0	pkg:pypi/packaging@25.0	Unknown, Apache-2.0, BSD-3 Clause, BSD-2 Clause	False	
pygments	2.19.2	pkg:pypi/pygments@2.19.2	Unknown, BSD-3 Clause, BSD-2 Clause	False	
requests	2.32.5	pkg:pypi/requests@2.32.5	Unknown, MIT, Apache-2.0	False	
snowballstemmer	3.0.1	pkg:pypi/snowballstemmer@3.0.1	BSD-3 Clause	False	
soupsieve	2.8	pkg:pypi/soupsieve@2.8	Unknown, MIT	False	
sphinx-basic-ng	1.0.0b2	pkg:pypi/sphinx-basic-ng@1.0.0b2	Unknown, MIT	False	
sphinx-copybutton	0.5.2	pkg:pypi/sphinx-copybutton@0.5.2	MIT	False	
sphinxcontrib-applehelp	2.0.0	pkg:pypi/sphinxcontrib-applehelp@2.0.0	BSD-3 Clause, BSD-2 Clause	False	
sphinxcontrib-devhelp	2.0.0	pkg:pypi/sphinxcontrib-devhelp@2.0.0	BSD-2 Clause	False	
sphinxcontrib-htmlhelp	2.1.0	pkg:pypi/sphinxcontrib-htmlhelp@2.1.0	BSD-2 Clause	False	
sphinxcontrib-jsmath	1.0.1	pkg:pypi/sphinxcontrib-jsmath@1.0.1	BSD-3 Clause, BSD-2 Clause	False	
sphinxcontrib-qthelp	2.0.0	pkg:pypi/sphinxcontrib-qthelp@2.0.0	BSD-3 Clause, BSD-2 Clause	False	
sphinxcontrib-serializinghtml	2.0.0	pkg:pypi/sphinxcontrib-serializinghtml@2.0.0	BSD-3 Clause, BSD-2 Clause	False	
typing-extensions	4.15.0	pkg:pypi/typing-extensions@4.15.0	BSD, BSD-3 Clause, GPL-1.0-or-later, Python-2.0	False	

[curator-admin]

+ Create Edit Remove



The screenshot shows the Occtet Curator SBOM Mgmt interface. The left sidebar contains navigation links: Dashboard, SBOM Mgmt (selected), Vulnerabilities, VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and Administration. The main area is titled 'SBOM Mgmt' and shows a project 'urlib-2.4.0'. The 'Inventory items' tab is active, displaying a table with one item: '20.35.3-75c946 (MIT)'. The table has columns: Resolved, ID, Aliases, Severity, Exploitability, and Risk score. The item has a risk score of 3.1. The right sidebar shows a list of vulnerabilities with their respective risk scores and status icons.

4.17.3.8 Python-dateutil-2.9.0.post0

<https://github.com/dateutil/dateutil>

Vulnerabilities: 15

The screenshot shows the Occtet Curator SBOM Mgmt interface for the project 'Python-dateutil - 2.9.0.post0'. The 'Inventory items' tab is active, displaying a table with 15 vulnerability items. The table has columns: Vulnerability, Risk score of vulnerability, and Number in software components. The items are listed with their respective risk scores and status icons. The right sidebar shows a list of vulnerabilities with their respective risk scores and status icons.



OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

SBOM Mgmt

Choose project

Pythin-dateutil - 2.9.0-post0

Search files...

Show all

Files

Overview

Inventory Items

Copyrights (0)

Licenses (5)

License	Number in software components
MPL 2.0	1
MIT	10
Apache 2.0	2
BSD-3-Clause	1
BSD-2-Clause	3

Vulnerabilities (15)

Create

Item

Files #

dateutil-master-5a1537 (NOASSERTION)	0
0.3.10-75c946 (Apache-2.0)	0
0.3.9-75c946 (BSD-3-Clause)	0
0.5.2-75c946 (MIT)	0
10.0.1-75c946 (MIT)	0
1.12.0-75c946 (MIT)	0
1.1.6-75c946 (BSD-2-Clause)	0
1.4.34-75c946 (MIT)	0
15.2.0-75c946 (MIT)	0
18.2.0-75c946 (MIT)	0
2.9.1-75c946 (MIT)	0
3.2.5-75c946 (MIT)	0
3.30.4-75c946 (MPL-2.0)	0
39.2.0-75c946 (MIT)	0
4.5.3-75c946 (Apache-2.0)	0
75c946-0.3.0 (NOASSERTION)	0
75c946-16.0 (NOASSERTION)	0
75c946-1.7.3.1.8.0.0-1.1.	0
75c946-21.1.0.0-21.1.0.0.	0
75c946-3.0 (NOASSERTION)	0
75c946-3.30 (NOASSERTION)	0
75c946-3.8.0 (NOASSERTION)	0
75c946-40.0 (NOASSERTION)	0
75c946 (NOASSERTION)	0
checkout-3..75c946.*.* (N..	0
checkout-4..75c946.*.* (N..	0
codecov-action-3..75c946...	0
cov-2.5.1-75c946 (BSD-2 Cla..	0
cov-75c946-2.0.0 (NOASS...	0

OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Vulnerabilities

Choose project

Pythin-dateutil - 2.9.0-f

Filter

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually cre...	Last update
VID-73n-jp05-widu	CVE-2026-22702, GHSA-977p-3phw-6986	Low	0.5	3.1	http://public.vulnerecode.io/vulnerabilities/VID-73n-jp05-widu	False	04/16/2026 13:28:51.036
VID-59he-2m2f-6uf6	CVE-2026-1703, GHSA-6vqw-5wp2-w6jp	Low	0.5	1.8	http://public.vulnerecode.io/vulnerabilities/VID-59he-2m2f-6uf6	False	04/16/2026 13:35:22.411
VID-ecwr-66f9-qk08	CVE-2025-8869, GHSA-4xn5-x5pr-qeph	Low	0.5	3.1	http://public.vulnerecode.io/vulnerabilities/VID-ecwr-66f9-qk08	False	04/16/2026 13:35:22.676
VID-fq7-5hyk-aaan	CVE-2018-20225	Low	0.5	3.5	http://public.vulnerecode.io/vulnerabilities/VID-fq7-5hyk-aaan	False	04/16/2026 13:35:22.821
VID-y54z-wzpf-aaas	BiT-2021-3572, BiT-pjp-2021-3572, CVE-2021-3572, GHSA-5qj3-jh3-5q8r, PYSEC-2021-437	Medium	0.5	4	http://public.vulnerecode.io/vulnerabilities/VID-y54z-wzpf-aaas	False	04/16/2026 13:35:23.121
VID-n88-avv0-aaas	CVE-2019-20916, GHSA-gpov-697-qwjl, PYSEC-2020-173, PYSEC-2020-192	Medium	0.5	4	http://public.vulnerecode.io/vulnerabilities/VID-n88-avv0-aaas	False	04/16/2026 13:35:23.392
VID-zv1y-y4fp-aaas	BiT-2023-5752, BiT-pjp-2023-5752, CVE-2023-5752, GHSA-m2t6-g339-26at, PYSEC-2023-228	Low	0.5	3.1	http://public.vulnerecode.io/vulnerabilities/VID-zv1y-y4fp-aaas	False	04/16/2026 13:35:23.649
VID-52y5-y9fq-aaan	CVE-2022-42969, GHSA-w596-4wvs-j96, PYSEC-2022-42969	Medium	0.5	4	http://public.vulnerecode.io/vulnerabilities/VID-52y5-y9fq-aaan	False	04/16/2026 13:35:26.165
VID-w93-p9d1-aaak	CVE-2020-29651, GHSA-t55x-574p-mj7c, PYSEC-2020-92	Medium	0.5	4	http://public.vulnerecode.io/vulnerabilities/VID-w93-p9d1-aaak	False	04/16/2026 13:35:26.336
VID-461-37zh-sqfy	BiT-virtualenv-2024-53899, CVE-2024-53899, GHSA-rq4-2hc7-8c8r, PYSEC-2024-187	Medium	0.5	4.4	http://public.vulnerecode.io/vulnerabilities/VID-461-37zh-sqfy	False	04/16/2026 13:35:27.366
VID-1c3j-k475-aaan	BiT-2022-40897, BiT-setuputils-2022-40897, CVE-2022-40897, GHSA-r8hw-vwmw-q578, PYSEC-0800-CVE-2022-40897, PYSEC-2022-43012	Medium	0.5	4	http://public.vulnerecode.io/vulnerabilities/VID-1c3j-k475-aaan	False	04/16/2026 13:35:28.710
VID-x2q-qv9r-g344	BiT-setuputils-2025-47273, CVE-2025-47273, GHSA-5qj3-jh3-5q8r, PYSEC-2025-49	Medium	0.5	4	http://public.vulnerecode.io/vulnerabilities/VID-x2q-qv9r-g344	False	04/16/2026 13:35:28.820
VID-pc2f-4k39-aaaa	CVE-2024-6343, GHSA-cv63-3mw6-8hw5	Medium	0.5	4	http://public.vulnerecode.io/vulnerabilities/VID-pc2f-4k39-aaaa	False	04/16/2026 13:35:28.890
VID-cq2r-k39-aaad	CVE-2013-1633, GHSA-27h4-476-jp5t, PYSEC-2013-32	Medium	0.5	4	http://public.vulnerecode.io/vulnerabilities/VID-cq2r-k39-aaad	False	04/16/2026 13:35:44.415
VID-m3de-waha-aaap	CVE-2011-4617, GHSA-39jc-wjgf-5fzc, PYSEC-2011-23	Low	0.5	3.1	http://public.vulnerecode.io/vulnerabilities/VID-m3de-waha-aaap	False	04/16/2026 13:35:52.881

Create

Edit

Remove

Excel

JSON



Occet Curator SBOM Mgmt

Choose project: **Python-dateutil - 2.9.0-post0**

Search files... Show all

Files

Overview **Inventory Items**

75c946- 40.0 (NOASSERTION)

Inventory item Vulnerabilities Files Audit notes Licenses Copyrights

Save

Filter

Resolved	ID	Aliases	Severity	Exploit
☐	VCID=02q-qvfr-g344	BIT-02q-qvfr-g344, CVE-2025-47273, GHSA-5jg-fvrg-3axf, PYSEC-2025-49	Medium	0.5
☐	VCID=1-cj-4475-aaan	BIT-2022-40897, BIT-02q-qvfr-g344, CVE-2022-40897, GHSA-rfth-vmmr-q579, PYSEC-0000-CVE-2022-40897, PYSEC-2022-43012	Medium	0.5
☐	VCID-cq2t-ncp-aaad	CVE-2013-1633, GHSA-27H4-J4T6-jp9f, PYSEC-2013-22	Medium	0.5
☐	VCID-pc7f-0k39-aaaa	CVE-2024-6345, GHSA-cx63-2mw6-8hw5	Medium	0.5

4 rows

Update vulnerabilities Create VEX

Item 10.0.1-75c946 (MIT) 1.4.34-75c946 (MIT) 15.2.0-75c946 (MIT) 39.2.0-75c946 (MIT) 75c946- 16.0 (NOASSERTION) 75c946- 40.0 (NOASSERTION)

Files #

[curator-admin] https://occtet.bitsea.de/boc/software-components

Occet Curator Software components

Choose project: **Python-dateutil - 2.9.0**

Filter

Name	Version	PURL	Licenses	Curated	License controlled by AI
actions/checkout	4.0.0	pkg:github/actions/checkout@4.0.0		False	
hypothesis	3.30	pkg:pypi/hypothesis		False	
build	0.3.0	pkg:pypi/build		False	
coverage	3.0	pkg:pypi/coverage		False	
pytest	2.0.0	pkg:pypi/pytest		False	
pytest-cov	2.0.0	pkg:pypi/pytest-cov		False	
attrs	21.1.0	pkg:pypi/attrs		False	
sphinx	1.7.3	pkg:pypi/sphinx		False	
readme-renderer	21.0	pkg:pypi/readme-renderer		False	
sphinx-rtd-theme	0.3.0	pkg:pypi/sphinx-rtd-theme		False	
pip	10.0.1	pkg:pypi/pip@10.0.1	MIT	False	
pluggy	0.5.2	pkg:pypi/pluggy@0.5.2	MIT	False	
enum34	1.1.6	pkg:pypi/enum34@1.1.6	BSD-2-Clause	False	
six	1.12.0	pkg:pypi/six@1.12.0	MIT	False	
colorama	0.3.9	pkg:pypi/colorama@0.3.9	BSD-3-Clause, BSD-2-Clause	False	
pytest-cov	2.5.1	pkg:pypi/pytest-cov@2.5.1	MIT, BSD-2-Clause	False	
pytest	3.2.5	pkg:pypi/pytest@3.2.5	MIT	False	
py	1.4.34	pkg:pypi/py@1.4.34	MIT	False	
freezegun	0.3.10	pkg:pypi/freezegun@0.3.10	Apache-2.0	False	
coverage	4.5.3	pkg:pypi/coverage@4.5.3	Apache-2.0	False	
virtualenv	15.2.0	pkg:pypi/virtualenv@15.2.0	MIT	False	
attrs	18.2.0	pkg:pypi/attrs@18.2.0	MIT	False	

33 rows

+ Create Edit Remove

[curator-admin]



4.17.3.9 Numpy-2.2.5

<https://github.com/numpy/numpy>

Vulnerabilities: 1

Resolved	ID	Allises	Severity	Exploitability	Risk score
☐	VCD-gsk8-3gqb-aaaa	CVE-2023-40590, GHSA-wfms-v35h-wvf4, PYSEC-0000-CVE-2023-40590, PYSEC-2023-161	Medium	0.5	4
☐	VCD-cpx1-8nzk-aaam	CVE-2023-41040, GHSA-cwvm-v4w8-q3lc, PYSEC-2023-165	Medium	0.5	4
☐	VCD-b8b-83ac-aaaf	CVE-2023-40267, GHSA-pr76-5cm5-w9qj, PYSEC-2023-137	Medium	0.5	4.5
☐	VCD-b1ur-48dr-aaaf	CVE-2024-02190, GHSA-2mqj-m65w-jghn, PYSEC-2024-4	Medium	0.5	4
☐	VCD-48et-5np-aaae	CVE-2023-24439, GHSA-hcqi-qp55-gfhn, PYSEC-0000-CVE-2023-24439, PYSEC-2023-42992	Medium	0.5	4.5



Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Vulnerabilities

Choose project

numpy - 2.2.5

> Filter

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
VCD-nyx2-1gpb-aaap	CVE-2015-4707, GHSA-66gw-5cof-qf5s, PYSEC-2017-46	Low	0.5	3.1	http://public.vulnsrcode.io/vulnerabilities/VCD-nyx2-1gpb-aaap	False	04/16/2026 13:44:39.637
VCD-46ad-5ngp-aaap	CVE-2022-24429, GHSA-hcgy-qd5f-qf5s, PYSEC-0000 CVE-2022-24429, PYSEC-2022-42992	Medium	0.5	4.5	http://public.vulnsrcode.io/vulnerabilities/VCD-46ad-5ngp-aaap	False	04/16/2026 13:45:00.153
VCD-b1u4-4bta-aaaf	CVE-2024-22190, GHSA-2mrg-m6fw-gphx, PYSEC-2024-4	Medium	0.5	4	http://public.vulnsrcode.io/vulnerabilities/VCD-b1u4-4bta-aaaf	False	04/16/2026 13:45:00.204
VCD-cxv1-8rta-aaam	CVE-2023-41040, GHSA-cvrm-v4ef-q58r, PYSEC-2023-165	Medium	0.5	4	http://public.vulnsrcode.io/vulnerabilities/VCD-cxv1-8rta-aaam	False	04/16/2026 13:45:00.247
VCD-gxk8-3qbp-aaaa	CVE-2023-40590, GHSA-wfm5-v35h-vw4f, PYSEC-0000 CVE-2023-40590, PYSEC-2023-161	Medium	0.5	4	http://public.vulnsrcode.io/vulnerabilities/VCD-gxk8-3qbp-aaaa	False	04/16/2026 13:45:00.291
VCD-br9-83ac-aaaf	CVE-2023-40267, GHSA-p76-5cm5-wkqj, PYSEC-2023-137	Medium	0.5	4.5	http://public.vulnsrcode.io/vulnerabilities/VCD-br9-83ac-aaaf	False	04/16/2026 13:45:00.361

[curator-admin] [+ Create](#) [Edit](#) [Remove](#) [Excel](#) [JSON](#)

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Software components

Choose project

numpy - 2.2.5

> Filter

Name	Version	PURL	Licenses	Curated	License controlled by AI
actions/checkout	de0fac2e4500abe0096e7214ff95547c0e30d	pkg:githubactions/actions/checkout@de0fac2e4500a...		False	
actions/setup-python	a309ff8b426b58ec9c2a45f08b6946889b02405	pkg:githubactions/actions/setup-python@a309ff8b42...		False	
actions/upload-artifact	bbca2da5da56ffaa83e35b676fdaaf77386f024f	pkg:githubactions/actions/upload-artifact@bbca2da5...		False	
astral-sh/setup-uv	cec208311d0545a65311c1a0d090b2062131e57	pkg:githubactions/astreal-sh/setup-uv@cec208311d05...		False	
github/codeql-action/init	c10b064d6d4919ea534254123db5e569572f13	pkg:githubactions/github/codeql-action/init@c10b06...		False	
github/codeql-action/analyze	c10b064d6d4919ea534254123db5e569572f13	pkg:githubactions/github/codeql-action/analyze@c10...		False	
github/codeql-action/autobuild	c10b064d6d4919ea534254123db5e569572f13	pkg:githubactions/github/codeql-action/autobuild@...		False	
ossf/scan-action	4eaa0f5438a392c3c463702b05e6e0c0e0f205a	pkg:githubactions/ossf/scan-action@4eaa0f54...		False	
github/codeql-action/upload-sarif	c10b064d6d4919ea534254123db5e569572f13	pkg:githubactions/github/codeql-action/upload-sarif...		False	
mpy	1.20.0	pkg:pypi/mpy@1.20.0		False	
pyrefly	0.6.0	pkg:pypi/pyrefly@0.6.0		False	
scipy-optim	0.3.31.188.0	pkg:pypi/scipy-optim@0.3.31.188.0		False	
scipy-optim	0.3.31.188.0	pkg:pypi/scipy-optim@0.3.31.188.0		False	
sphinx-design		pkg:pypi/sphinx-design		False	
twocli		pkg:pypi/twocli		False	
matplotlib	< 3.10.6 > 3.10.6	pkg:pypi/matplotlib		False	
sphinx	7.2.6	pkg:pypi/sphinx@7.2.6	BSD-3-Clause, BSD-2-Clause	False	
sphinx-copybutton		pkg:pypi/sphinx-copybutton		False	
jupyterlab-proxide-kernel	0.5.2	pkg:pypi/jupyterlab-proxide-kernel@0.5.2	BSD-3-Clause	False	
jupyterlab-sphinx	>= 0.10.0	pkg:pypi/jupyterlab-sphinx		False	
numpydoc	1.10.0	pkg:pypi/numpydoc@1.10.0	MIT, BSD-2-Clause	False	
lythion	< 8.1.0 > 8.1.0	pkg:pypi/lythion		False	

[curator-admin] [+ Create](#) [Edit](#) [Remove](#)



4.17.3.10 Packaging-25.0

<https://github.com/pypa/packaging>

The screenshot shows the Occtet Curator SBOM Mgmt interface. The left sidebar contains navigation links: Dashboard, SBOM Mgmt, Vulnerabilities, VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and Administration. The main content area is titled 'SBOM Mgmt' and shows the 'Overview' tab for the project 'PyPa - 25.0'. The 'Overview' tab displays a table with columns 'Copyright name' and 'Number in files'. Below this table, there are sections for 'Licenses (0)' and 'Vulnerabilities (0)'. On the right side, there is a '+ Create' button and a list of files with their names and file counts.

The screenshot shows the Occtet Curator Vulnerabilities interface. The left sidebar contains navigation links: Dashboard, SBOM Mgmt, Vulnerabilities, VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and Administration. The main content area is titled 'Vulnerabilities' and shows a table for the project 'PyPa - 25.0'. The table has columns: ID, Aliases, Severity, Exploitability, Risk score, Source URL, Manually created, and Last update. At the bottom of the table, there are buttons for '+ Create', 'Edit', and 'Remove'. On the right side, there are buttons for 'Excel' and 'JSON'.

The screenshot displays the 'Octet Curator' web application. The left sidebar contains navigation links: Dashboard, SBOM Mgmt, Vulnerabilities, VEX listing, Projects, Software components (highlighted), Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and Administration.

The main content area is titled 'Software components'. It features a 'Choose project' dropdown menu set to 'PyPa - 25.0'. Below this is a 'Filter' button. A table lists software components with columns: Name, Version, PURL, Licenses, Curated, and License controlled by AI. The table contains 10 rows of data.

Name	Version	PURL	Licenses	Curated	License controlled by AI
actions/checkout	d6f9c3a4506aba009e47214ff55447ce83d0	pkg.github.com/actions/checkout@d6f9c3a4506a...		False	
actions/setup-python	a309fb4c4b05fec02a45096be946889e0c405	pkg.github.com/actions/setup-python@a309fb4c...		False	
actions/download-artifact	3a5645dc0d9172054a40b74d9db05a5447a7c	pkg.github.com/actions/download-artifact@3a56...		False	
actions/upload-artifact	b8bc4dd69a56ffeeaf3a76b766aa773868024f	pkg.github.com/actions/upload-artifact@b8bc4d...		False	
py-pa-gh-action-publish	e0fc53931016c89c32cb73a98c7867648fa027a	pkg.github.com/py-pa-gh-action-publish@e0fc5...		False	
github/codeql-actions/analyze	89a394ae59626350863aa6b04252a67ae50cfe3e	pkg.github.com/github/codeql-actions/analyze@89...		False	
github/codeql-actions/init	89a394ae59626350863aa6b04252a67ae50cfe3e	pkg.github.com/github/codeql-actions/init@89a3...		False	
github/codeql-actions/autobuild	89a394ae59626350863aa6b04252a67ae50cfe3e	pkg.github.com/github/codeql-actions/autobuild@89...		False	
astral-sh/setup-or	37802ad634d732d68d71619e30fd234e172b78	pkg.github.com/astral-sh/setup-or@37802ad634...		False	
re-actors/allis-green	05ac93880fwebcs572faf17fcccdcf8efcc5fe	pkg.github.com/re-actors/allis-green@05ac9388...		False	
invoke		pypi/invoke		False	
com.github.py-pa-packaging	main	pypi/com.github.py-pa-packaging/main		False	

At the bottom of the page, there are three buttons: '+ Create', 'Edit', and 'Remove'.

Octet Curator

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components

Choose project

Alamofire - 1.0

> Filter

Name

Version

PURL

Licenses

Curated

License controlled by AI

CFPropertyList	3.0.8	pkg:gem/CFPropertyList@3.0.8		False	
actions/checkout	v6	pkg:github/actions/checkout@v6		False	
activesupport	7.2.3.1	pkg:gem/activesupport@7.2.3.1		False	
addressable	2.9.0	pkg:gem/addressable@2.9.0		False	
algoliasearch	1.27.5	pkg:gem/algoliasearch@1.27.5		False	
atomos	0.1.3	pkg:gem/atomos@0.1.3		False	
base64	0.3.0	pkg:gem/base64@0.3.0		False	
benchmark	0.5.0	pkg:gem/benchmark@0.5.0		False	
bigdecimal	4.1.1	pkg:gem/bigdecimal@4.1.1		False	
cladej	1.1.0	pkg:gem/cladej@1.1.0		False	
cocapods	1.16.2	pkg:gem/cocapods@1.16.2		False	
cocapods-core	1.16.2	pkg:gem/cocapods-core@1.16.2		False	
cocapods-deintegrate	1.0.5	pkg:gem/cocapods-deintegrate@1.0.5		False	
cocapods-downloader	2.1	pkg:gem/cocapods-downloader@2.1		False	
cocapods-plugins	1.0.0	pkg:gem/cocapods-plugins@1.0.0		False	
cocapods-search	1.0.1	pkg:gem/cocapods-search@1.0.1		False	
cocapods-trunk	1.6.0	pkg:gem/cocapods-trunk@1.6.0		False	
cocapods-try	1.2.0	pkg:gem/cocapods-try@1.2.0		False	
colored2	3.1.2	pkg:gem/colored2@3.1.2		False	
compnred/gha-setup-swift	main	pkg:github/compnred/gha-setup-swift@main		False	
concurrent-ruby	1.3.6	pkg:gem/concurrent-ruby@1.3.6		False	
connection_pool	3.0.2	pkg:gem/connection_pool@3.0.2		False	

+ Create

Edit

Remove



Octet Curator

SBOM Mgmt

Choose project: **Alamofire - 1.0**

Search files... **0.0**

Show all

Files

- dependencies
 - checkout
 - v5
 - licenses
 - ngm
 - @actions
 - core.dep.yml
 - exec.dep.yml
 - github.dep.yml
 - http-client.dep.yml
 - io.dep.yml
 - tool-cache.dep.yml
 - @fastify
 - busboy.dep.yml
 - @octokit
 - auth-token.dep.yml
 - core.dep.yml
 - endpoint.dep.yml
 - graphql.dep.yml
 - openapi-types 20.0.0.dep.yml
 - openapi-types 22.1.0.dep.yml
 - plugin-paginate-rest.dep.yml
 - plugin-rest-endpoint-methods.dep.yml
 - request-error.dep.yml
 - request.dep.yml

Overview Files

> Copyrights (0)

> Licenses (0)

> Vulnerabilities (1)

Vulnerability	Risk score of vulnerability	Number in software compon...
VCD-yjt-rs24-dtz	2.4	1

Item Files #

- \github\workflows\ci.yml 1
- \gemfile.lock 1
- C:\Users\Jithendra.Palepu\Downloads\Alamofire-5.1.1.2 (NOASSERTION) 0
- action actions-checkout-d26bae245f1b4aaav (NOASSERTION) 0
- action comperd-gha-setup-swift-0502f50e1825e9e7main (NOASSER... 0
- action github-codeql-action-analyze-366ec2ad8b39661v4 (NOASSER... 0
- action github-codeql-action-init-bc8f8a32450e3d1v4 (NOASSER... 0
- action skiptrails-swift-android action-ba1dec7976786762v2 (NOASS... 0
- activesupport-42b4c7dcb8a0747.2.3.1 (NOASSERTION) 0
- addressable-e1bf2bc1c38e7c802.9.0 (NOASSERTION) 0
- algolia-search-7b75ed0e8559ab6e1.27.5 (NOASSERTION) 0
- atomos-385981ad88f38870.1.3 (NOASSERTION) 0
- base64-d77b45a473282ac70.3.0 (NOASSERTION) 0
- benchmark-31bc7f5a8e33a3d30.5.0 (NOASSERTION) 0
- bigdecimal-920af01c1b386ccc4.1.1 (NOASSERTION) 0
- CSPPropertyList-7208ad0b1871e893.0.8 (NOASSERTION) 0
- claiide-9c3754daefc750801.1.0 (NOASSERTION) 0
- cocopods-trunk-e0849148398679a61.6.0 (NOASSERTION) 0
- cocopods-core-e72d855de671d1d1.16.2 (NOASSERTION) 0
- cocopods-deintegrate-364924c1195590c1.0.5 (NOASSERTION) 0
- cocopods-downloader-faf5c7f1d92a034052.1 (NOASSERTION) 0
- cocopods-plugins-51e740120490e91.0.0 (NOASSERTION) 0
- cocopods-search-c40945a07439ca851.0.1 (NOASSERTION) 0
- cocopods-trunk-e0849148398679a61.6.0 (NOASSERTION) 0
- cocopods-try-45e050581141f1c11.2.0 (NOASSERTION) 0
- colored2-3362b2c3c0e6f9b43.1.2.0 (NOASSERTION) 0
- concurrent-ruby-3a091c313c2e4dc1.3.6 (NOASSERTION) 0
- connection-pool-ac70d6c95c5d0563.0.2 (NOASSERTION) 0
- dtb-c1520f48358f6632.2.3 (NOASSERTION) 0

Octet Curator

Vulnerabilities

Choose project: **Alamofire - 1.0**

> Filter

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
VCD-yjt-rs24-dtz	CVE-2025-58767, GHSA-c2t4-jmnc-qd75	Low	0.5	2.4	http://public.vulnabrillcode.io/vulnerabilities/VCD-yjt-rs24-dtz	False	04/15/2026 13:39 18.659

1 row

localhost:8090/boc/dashboard-view

+ Create Edit Remove

Excel JSON



4.17.4.2 Vapor

<https://github.com/vapor/vapor>



Octet Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Vulnerabilities

Choose project
vapor - 1.0

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

[admin]

+ Create

Edit

Remove

Excel

JSON

Octet Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Software components

Choose project
vapor - 1.0

> Filter

<< 38 rows >>

Name	Version	PURL	Licenses	Curated	License controlled by AI
github.com/apple/swift-http-structured-headers	1.6.0	pkg:swift/github.com/apple/swift-http-structured-hea...		False	
github.com/apple/swift-distributed-tracing	1.4.1	pkg:swift/github.com/apple/swift-distributed-tracing...		False	
github.com/apple/swift-algorithms	1.2.1	pkg:swift/github.com/apple/swift-algorithms@1.2.1		False	
github.com/apple/swift-nio-transport-services	1.26.0	pkg:swift/github.com/apple/swift-nio-transport-serv...		False	
github.com/apple/swift-configuration	1.2.0	pkg:swift/github.com/apple/swift-configuration@1.2.0		False	
github.com/vapor/multipart-kit	4.7.1	pkg:swift/github.com/vapor/multipart-kit@4.7.1		False	
github.com/apple/swift-certificates	1.18.0	pkg:swift/github.com/apple/swift-certificates@1.18.0		False	
github.com/apple/swift-nio-ssl	2.36.1	pkg:swift/github.com/apple/swift-nio-ssl@2.36.1		False	
github.com/swift-server/async-http-client	1.33.1	pkg:swift/github.com/swift-server/async-http-clien...		False	
github.com/apple/swift-collections	1.4.1	pkg:swift/github.com/apple/swift-collections@1.4.1		False	
github.com/vapor/console-kit	4.16.0	pkg:swift/github.com/vapor/console-kit@4.16.0		False	
github.com/apple/swift-nio-extras	1.33.0	pkg:swift/github.com/apple/swift-nio-extras@1.33.0		False	
github.com/swift-server/swift-service-lifecycle	2.11.0	pkg:swift/github.com/swift-server/swift-service-lifecy...		False	
github.com/apple/swift-log	1.11.0	pkg:swift/github.com/apple/swift-log@1.11.0		False	
github.com/apple/swift-numerics	1.1.1	pkg:swift/github.com/apple/swift-numerics@1.1.1		False	
github.com/apple/swift-metrics	2.8.0	pkg:swift/github.com/apple/swift-metrics@2.8.0		False	
github.com/apple/swift-nio-http2	1.42.0	pkg:swift/github.com/apple/swift-nio-http2@1.42.0		False	
github.com/vapor/routing-kit	4.9.3	pkg:swift/github.com/vapor/routing-kit@4.9.3		False	
github.com/apple/swift-async	1.6.0	pkg:swift/github.com/apple/swift-async@1.6.0		False	
github.com/apple/swift-service-context	1.3.0	pkg:swift/github.com/apple/swift-service-context@1...		False	
github.com/apple/swift-crypto	4.3.1	pkg:swift/github.com/apple/swift-crypto@4.3.1		False	
github.com/apple/swift-atomics	1.3.0	pkg:swift/github.com/apple/swift-atomics@1.3.0		False	

[admin]

+ Create

Edit

Remove



4.17.4.3 ReactiveX

<https://github.com/ReactiveX/RxSwift>

Vulnerabilities: 5

Octet Curator SBOM Mgmt

Choose project: **ReactiveX_RxSwift - e5acc1**

Search files... Show all

Overview Inventory items

> Copyrights (0)

> Licenses (5)

License	Number in software components
MIT	22
BSD-3 Clause	2
Apache-2.0	2
Ruby	2
LGPL-2.1-or-later	1

> Vulnerabilities (5)

Files

Item	Files #
RxSwift-main-93497a (MIT)	0
0.0.4-75c946 (BSD-2-Clause OR ...)	0
0.1.2-75c946 (MIT)	0
0.3.0-75c946 (MIT)	0
0.8.2-75c946 (MIT)	0
1.0.3-75c946 (MIT)	0
1.1.0-75c946 (MIT)	0
1.13.1-75c946 (MIT)	0
1.3.4-75c946 (Ruby)	0
1.4.1-75c946 (MIT)	0
1.8.0-75c946 (LGPL-2.1-or-later)	0
2.3.1-75c946 (MIT)	0
2.8.0-75c946 (Apache-2.0)	0
3.1.2-75c946 (MIT)	0
3.4.4-75c946 (BSD-2-Clause ANL...)	0
4.0.6-75c946 (MIT)	0
4.21.0-75c946 (MIT)	0
8.2.3-75c946 (MIT)	0
checkout3...75c9463** (NOAS...)	0
checkout4...75c9464** (NOAS...)	0
displaywidth-1.7.0-75c946 (MIT)	0
excon-1.1.0-75c946 (MIT)	0
http-cache-2.2.0-75c946 (Apach...)	0
nethttp-1.0.1-75c946 (MIT)	0
nethttpersistent-1.1.0-75c946 (...)	0
parser-gfm-1.1.0-75c946 (MIT)	0
plugins-0.9.2-75c946 (MIT)	0
post-2.1.1-75c946 (MIT)	0

Octet Curator SBOM Mgmt

Choose project: **ReactiveX_RxSwift - e5acc1**

Search files... Show all

Overview Inventory items

> Copyrights (0)

> Licenses (5)

> Vulnerabilities (5)

Vulnerability	Risk score of vulnerability	Number in software components
VCD-4jft-r24-tdtz	2.4	1
VCD-kfaf-yq3-gpog	3.1	1
VCD-mck9-nedv-aaam	4.4	1
VCD-fnw0-akjv-aaah	4	1
VCD-d35k-r223-aaaj	1.5	1

Files

Item	Files #
RxSwift-main-93497a (MIT)	0
0.0.4-75c946 (BSD-2-Clause OR ...)	0
0.1.2-75c946 (MIT)	0
0.3.0-75c946 (MIT)	0
0.8.2-75c946 (MIT)	0
1.0.3-75c946 (MIT)	0
1.1.0-75c946 (MIT)	0
1.13.1-75c946 (MIT)	0
1.3.4-75c946 (Ruby)	0
1.4.1-75c946 (MIT)	0
1.8.0-75c946 (LGPL-2.1-or-later)	0
2.3.1-75c946 (MIT)	0
2.8.0-75c946 (Apache-2.0)	0
3.1.2-75c946 (MIT)	0
3.4.4-75c946 (BSD-2-Clause ANL...)	0
4.0.6-75c946 (MIT)	0
4.21.0-75c946 (MIT)	0
8.2.3-75c946 (MIT)	0
checkout3...75c9463** (NOAS...)	0
checkout4...75c9464** (NOAS...)	0
displaywidth-1.7.0-75c946 (MIT)	0
excon-1.1.0-75c946 (MIT)	0
http-cache-2.2.0-75c946 (Apach...)	0
nethttp-1.0.1-75c946 (MIT)	0
nethttpersistent-1.1.0-75c946 (...)	0
parser-gfm-1.1.0-75c946 (MIT)	0
plugins-0.9.2-75c946 (MIT)	0
post-2.1.1-75c946 (MIT)	0



 Occtet Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

SBOM Mgmt

Choose project

ReactiveX_RxSwift - e5acc1

Search files...

Show all

Files

Overview

Inventory items

Inventory item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Inventory name

1.4.1-75c946 (MIT)

Parent inventory item

RxSwift-main-93497a (MIT)

Software component

faraday

Download URL

NOASSERTION

Download

Linking

Priority

Number of files

Curated

Created at

04/16/2026 11:18:31:067

+ Create

Vulnerable X

Item

Files #

1.4.1-75c946 (MIT)

0

2.3.1-75c946 (MIT)

0

3.8.0-75c946 (Apache 2.0)

0

3.4.4-75c946 (BSD-2 Clause AND ML)

0

4.21.0-75c946 (MIT)

0

SBOM Mgmt

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT Issues
ORT Violation
Import
Help
Administration
Configuration
Organizations
Services
Users
Backend logs

Choose project
ReactiveX_RxSwift - e5acc1

Search files...
Show all

Files

Overview
Inventory items

1.4.1-75c946 (MIT)

Inventory item
Vulnerabilities
Files
Audit notes
Licenses
Copyrights

Save

Filter

Resolved	ID	Aliases	Severity	Exploitability	Risk score
	VCID-kfak-97c3-gqag	CVE-2026-23765, GHSA-33mh-2634-fwf2	Low	0.5	3.1

Update vulnerabilities
Create VEX

Vulnerable

Item
Files

1.4.1-75c946 (MIT)	0	
2.3.1-75c946 (MIT)	0	
2.8.0-75c946 (Apache 2.0)	0	
3.4.4-75c946 (BSD-2-Clause AND ML_	0	
4.21.0-75c946 (MIT)	0	



OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

Vulnerabilities

Choose project

:liveX_RxSwift - e5acc1

> Filter

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
YCID-xft-vc34-8ftz	CVE-2025-58767, DHS&C2H4-gmrc-qd5	Low	0.5	2.4	http://public.vulnablenode.io/vulnerabilities/YCID-xft-vc34-8ftz	False	04/16/2026 10:31:00.624
YCID-rlaf-vrc3-gorg	CVE-2026-25765, DHS&C2H4-2634-fwr2	Low	0.5	2.1	http://public.vulnablenode.io/vulnerabilities/YCID-rlaf-vrc3-gorg	False	04/16/2026 10:32:19.998
YCID-mdk9-edv9-aasm	CVE-2021-28834, DHS&C2H4-v744-nwaj	Medium	0.5	4.4	http://public.vulnablenode.io/vulnerabilities/YCID-mdk9-edv9-aasm	False	04/16/2026 11:18:35.524
YCID-fmw6-akj9-aash	CVE-2021-32740, DHS&C2H4-q857-3jkg	Medium	0.5	4	http://public.vulnablenode.io/vulnerabilities/YCID-fmw6-akj9-aash	False	04/16/2026 11:18:45.586
YCID-433k-v323-aaaj	CVE-2022-31072, DHS&C2H4-pg3-qgn8	Low	0.5	1.5	http://public.vulnablenode.io/vulnerabilities/YCID-433k-v323-aaaj	False	04/16/2026 11:18:48.159

[admin]

+ Create

Edit

Remove

Excel

JSON

OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

Software components

Choose project

:liveX_RxSwift - e5acc1

> Filter

Name	Version	PURL	Licenses	Curated	License controlled by AI
colored2	3.1.2	pkg:gem/colored2@3.1.2	MIT	False	
rexml	3.4.4	pkg:gem/rexml@3.4.4	MIT, BSD-2-Clause	False	
nap	1.1.0	pkg:gem/nap@1.1.0	MIT	False	
faraday-escon	1.1.0	pkg:gem/faraday-escon@1.1.0	MIT	False	
actions/checkout	4.**	pkg:github/actions/actions/checkout@4.32A.32A		False	
multipart-post	2.1.1	pkg:gem/multipart-post@2.1.1	MIT	False	
no_proxy_fix	0.1.2	pkg:gem/no_proxy_fix@0.1.2	MIT	False	
faraday	1.4.1	pkg:gem/faraday@1.4.1	MIT	False	
krandown	2.3.1	pkg:gem/krandown@2.3.1	MIT	False	
git	1.13.1	pkg:gem/git@1.13.1	MIT	False	
faraday-http-cache	2.2.0	pkg:gem/faraday-http-cache@2.2.0	Apache-2.0	False	
faraday-net_http	1.0.1	pkg:gem/faraday-net_http@1.0.1	MIT	False	
unicode-display_width	1.7.0	pkg:gem/unicode-display_width@1.7.0	MIT	False	
sawyer	0.8.2	pkg:gem/sawyer@0.8.2	MIT	False	
clalde-plugins	0.9.2	pkg:gem/clalde-plugins@0.9.2	MIT	False	
cork	0.3.0	pkg:gem/cork@0.3.0	MIT	False	
rchardev	1.8.0	pkg:gem/rchardev@1.8.0	LGPL 2.1 or later	False	
clalde	1.0.3	pkg:gem/clalde@1.0.3	MIT	False	
danger	8.2.3	pkg:gem/danger@8.2.3	MIT	False	
addressable	2.8.0	pkg:gem/addressable@2.8.0	Apache-2.0	False	
open4	1.3.4	pkg:gem/open4@1.3.4	Ruby	False	
faraday-net_http_persistent	1.1.0	pkg:gem/faraday-net_http_persistent@1.1.0	MIT	False	
...	...	...	...	...	...

[admin]

+ Create

Edit

Remove



4.17.4.4 Kingfisher

<https://github.com/onevcat/Kingfisher>

Vulnerabilities: 1

Octet Curator SBOM Mgmt

Choose project: **Onevcat_Kingfisher - 483094**

Search files... Show all

Licenses (10)

License	Number in software components
BSD-2-Clause	17
GPL-2.0-only	1
MPL-2.0	1
Ruby	18
ISC	1
Unknown	2
JSON	1
MIT	84
Apache 2.0	17

Vulnerabilities (1)

Vulnerability	Risk score of vulnerability	Number in software components
VCD-4jR-r24-0bZ	2.4	1

Files

Item	Files #
Kingfisher-master-bed703 (MIT)	0
0.0.20-75c946 (MIT)	0
0.0.4-75c946 (BSD-3-Clause)	0
0.0.5-75c946 (BSD-2-Clause OR ...)	0
0.1.0-75c946 (MIT)	0
0.1.2-75c946 (BSD-2-Clause OR ...)	0
0.1.3-75c946 (MIT)	0
0.1.5-75c946 (MIT)	0
0.11.0-75c946 (MIT)	0
0.112.0-75c946 (MIT)	0
0.18.0-75c946 (MIT)	0
0.2.0-75c946 (BSD-2-Clause A...)	0
0.2.0-75c946 (BSD-2-Clause OR ...)	0
0.21.0-75c946 (Apache-2.0)	0
0.3.0-75c946 (BSD-2-Clause A...)	0
0.4.0-75c946 (MIT)	0
0.4.1-75c946 (BSD-2-Clause A...)	0
0.4.1-75c946 (MIT)	0
0.5.0-75c946 (BSD-2-Clause A...)	0
0.6.20240107-75c946 (BSD-3 Cl...)	0
0.6.3-75c946 (BSD-2-Clause A...)	0
0.8.0-75c946 (MIT)	0
0.8.1-75c946 (BSD-2-Clause A...)	0
1.0.0-75c946 (MIT)	0
1.0.4-75c946 (MIT)	0
1.0.5-75c946 (ISC)	0
1.1.0-75c946 (MIT)	0
1.1.3-75c946 (MIT)	0

Octet Curator SBOM Mgmt

Choose project: **Onevcat_Kingfisher - 483094**

Search files... Show all

Vulnerabilities (1)

Vulnerability	Risk score of vulnerability	Number in software components
VCD-4jR-r24-0bZ	2.4	1

Files

Item	Files #
Kingfisher-master-bed703 (MIT)	0
0.0.20-75c946 (MIT)	0
0.0.4-75c946 (BSD-3-Clause)	0
0.0.5-75c946 (BSD-2-Clause OR ...)	0
0.1.0-75c946 (MIT)	0
0.1.2-75c946 (BSD-2-Clause OR ...)	0
0.1.3-75c946 (MIT)	0
0.1.5-75c946 (MIT)	0
0.11.0-75c946 (MIT)	0
0.112.0-75c946 (MIT)	0
0.18.0-75c946 (MIT)	0
0.2.0-75c946 (BSD-2-Clause A...)	0
0.2.0-75c946 (BSD-2-Clause OR ...)	0
0.21.0-75c946 (Apache-2.0)	0
0.3.0-75c946 (BSD-2-Clause A...)	0
0.4.0-75c946 (MIT)	0
0.4.1-75c946 (BSD-2-Clause A...)	0
0.4.1-75c946 (MIT)	0
0.5.0-75c946 (BSD-2-Clause A...)	0
0.6.20240107-75c946 (BSD-3 Cl...)	0
0.6.3-75c946 (BSD-2-Clause A...)	0
0.8.0-75c946 (MIT)	0
0.8.1-75c946 (BSD-2-Clause A...)	0
1.0.0-75c946 (MIT)	0
1.0.4-75c946 (MIT)	0
1.0.5-75c946 (ISC)	0
1.1.0-75c946 (MIT)	0
1.1.3-75c946 (MIT)	0



OCCTET Curator

SBOM Mgmt

Choose project

Onevcat_Kingfisher - 483094

Search files...

Show all

Files

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

SBOM Mgmt

Overview

Inventory items

3.4.4-75c946 ((BSD-2-Clause AND MIT))

Inventory item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Create

Item

Files

3.4.4-75c946 ((BSD-2-Clause AND MIT))

0

0

Inventory name

3.4.4-75c946 ((BSD-2-Clause AND MIT))

Parent inventory item

Kingfisher-master-bed703 (MIT)

Software component

rexml

Download URL

NOASSERTION

Linking

Priority

Number of files

0

Curated

Created at: 04/16/2026 11:11:04:762

OCCTET Curator

SBOM Mgmt

Choose project

Onevcat_Kingfisher - 483094

Search files...

Show all

Files

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

SBOM Mgmt

Overview

Inventory items

3.4.4-75c946 ((BSD-2-Clause AND MIT))

Inventory item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Create

Item

Files

3.4.4-75c946 ((BSD-2-Clause AND MIT))

0

0

Filter

Resolved

ID

Aliases

Severity

Exploitability

Risk score

1

row

Resolved

ID

Aliases

Severity

Exploitability

Risk score

0

VDB-2024-0124

CVE-2025-58767, GHSA-c214-gmcc-q2t5

Low

0.5

2.4

Update vulnerabilities

Create VEX



Octet Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

Software components

Choose project
at_Kingfisher - 483094

> Filter

Name	Version	PURL	Licenses	Curated	License controlled by AI
gh_inspector	1.1.3	pkg:gem/gh_inspector@1.1.3	MIT	False	
artifactory	3.0.17	pkg:gem/artifactory@3.0.17	Apache 2.0	False	
excon	0.112.0	pkg:gem/excon@0.112.0	MIT	False	
googleauth	1.11.2	pkg:gem/googleauth@1.11.2	Apache 2.0	False	
csv	3.3.5	pkg:gem/csv@3.3.5	Ruby, BSD-2-Clause, MIT	False	
http-cookie	1.0.8	pkg:gem/http-cookie@1.0.8	MIT	False	
colored2	3.1.2	pkg:gem/colored2@3.1.2	MIT	False	
xcodproj	1.27.0	pkg:gem/xcodproj@1.27.0	MIT	False	
faraday-ems-synchrony	1.0.1	pkg:gem/faraday-ems-synchrony@1.0.1	MIT	False	
rexml	3.4.4	pkg:gem/rexml@3.4.4	MIT, BSD-2-Clause	False	
atomos	0.1.3	pkg:gem/atomos@0.1.3	MIT	False	
commander	4.6.0	pkg:gem/commander@4.6.0	MIT	False	
nap	1.1.0	pkg:gem/nap@1.1.0	MIT	False	
domain_name	0.5.20240107	pkg:gem/domain_name@0.5.20240107	BSD-3-Clause, MPL 2.0, BSD-2-Clause	False	
nanaimo	0.4.0	pkg:gem/nanaimo@0.4.0	MIT	False	
public_suffix	4.0.7	pkg:gem/public_suffix@4.0.7	MIT	False	
cocopods-plugins	1.0.0	pkg:gem/cocopods-plugins@1.0.0	MIT	False	
sysrandom	1.0.5	pkg:gem/sysrandom@1.0.5	ISC	False	
bigdecimal	4.1.0	pkg:gem/bigdecimal@4.1.0	BSD-2-Clause, Ruby	False	
emoji_regex	3.2.3	pkg:gem/emoji_regex@3.2.3	MIT	False	
abbrev	0.1.2	pkg:gem/abbrev@0.1.2	BSD-2-Clause, Ruby	False	
naturally	2.3.0	pkg:gem/naturally@2.3.0	MIT	False	

+ Create

Edit

Remove

[admin]

Octet Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

Vulnerabilities

Choose project
at_Kingfisher - 483094

> Filter

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
VOD-yjfr-rs24-dbfz	CVE-2025-58767, GHSA-c154-jgmc-q7t5	Low	0.5	2.4	http://public-vulnerabilitycode.io/vulnerabilities/VOD-yjfr-rs24-dbfz	False	04/16/2025 10:31:00:624

+ Create

Edit

Remove

[admin]

Export

JSON



4.17.4.5 SwiftyJSON

<https://github.com/SwiftyJSON/SwiftyJSON>



4.17.4.6 Snapkit

<https://github.com/SnapKit/SnapKit>

The screenshot displays the Occtet Curator web application interface. The top navigation bar includes a sidebar with various menu items: Dashboard, SBOM Mgmt, Vulnerabilities, VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and Administration. The main content area is divided into two sections: 'Vulnerabilities' and 'SBOM Mgmt'.

Vulnerabilities Section: This section shows a table with columns for ID, Aliases, Severity, Exploitability, Risk score, Source URL, Manually created, and Last update. The table is currently empty. Below the table, there are buttons for '+ Create', 'Edit', and 'Remove'. At the bottom right, there are buttons for 'Excl' and 'JSON'.

SBOM Mgmt Section: This section is divided into two sub-sections: 'Overview' and 'Inventory items'. The 'Inventory items' sub-section is active, showing a form for creating a new inventory item. The form includes fields for 'Inventory name' (SnapKit-develop-1aeb3f (MIT)), 'Parent inventory item' (a dropdown menu), 'Software component' (com.github.SnapKit/SnapKit), and 'Download URL' (git+https://github.com/SnapKit/SnapKit). There are also fields for 'Linking', 'Priority', and 'Number of files' (0). A 'Curated' checkbox is present. A 'Save' button is located at the bottom right of the form. The 'Created at' timestamp is 04/16/2026 09:57:27:200.



4.17.4.7 Moya

<https://github.com/Moya/Moya>

Vulnerabilities: 14

The screenshot shows the 'Occtet Curator' interface with the 'SBOM Mgmt' section selected. The 'Vulnerabilities' tab is active, displaying a list of 14 vulnerabilities for the project 'Moya - 418d53'. The table includes columns for 'Vulnerability', 'Risk score of vulnerability', and 'Number in software components'. The vulnerabilities listed are:

Vulnerability	Risk score of vulnerability	Number in software components
VCD-9mm-q5d-hq5	4	1
VCD-yft-rs24-dt5	2.4	1
VCD-rlaf-rq2-q0q	3.1	1
VCD-9lrv-q3kw-aaak	4	1
VCD-fhw8-akj-aaah	4	1
VCD-caw7-q3k-aaas	3.4	1
VCD-eh4-cqwc-aaah	3.1	1
VCD-xpw5-y7b-aaag	3.1	1
VCD-4da-29mt-y7q	3.4	1

On the right side, there is a list of files with their respective vulnerability status and risk scores. The files listed are:

Item	Files #
Moya-master-ea82d4 (MIT)	0
0.0.4-75c946 (BSD-3-Clause)	0
0.0.5-75c946 ((BSD-2-Clause A...	0
0.1.3-75c946 (MIT)	0
0.11.0-75c946 (MIT)	0
0.15.0-75c946 (MIT)	0
0.3.0-75c946 (MIT)	0
0.8.0-75c946 (MIT)	0
0.9.2-75c946 (MIT)	0
1.1.0-75c946 (MIT)	0
1.1.3-75c946 (MIT)	0
1.11.3-75c946 (MIT)	0
1.12.0-75c946 (MIT)	0
1.15.5-75c946 (BSD-3-Clause A...	0
1.22.0-75c946 (MIT)	0
1.27.5-75c946 (MIT)	0
1.4.0-75c946 (MIT)	0
13.0.6-75c946 (MIT)	0
2.0.4-75c946 (MIT)	0
2.0.5-75c946 (MIT)	0
2.0.7-75c946 ((BSD-2-Clause OR ...	0
2.3.1-75c946 (MIT)	0
2.5.2-75c946 (MIT)	0
2.6.0-75c946 (MIT)	0
2.6.2-75c946 ((Ruby OR (BSD-2-...	0
2.8.0-75c946 (Apache 2.0)	0
2.8.3-75c946 (Ruby)	0
3.0.5-75c946 (MIT)	0

The screenshot shows the 'Occtet Curator' interface with the 'SBOM Mgmt' section selected. The 'Vulnerabilities' tab is active, displaying the details of a specific vulnerability: '2.0.5-75c946 (MIT)'. The details include:

- Inventory name:** 2.0.5-75c946 (MIT)
- Parent inventory item:** Moya-master-ea82d4 (MIT)
- Software component:** tzinfo
- Download URL:** NOASSERTION
- Linking:** (Dropdown menu)
- Priority:** (Dropdown menu)
- Number of files:** 0
- Curated:** (Checkbox)

On the right side, there is a list of files with their respective vulnerability status and risk scores. The files listed are:

Item	Files #
2.0.5-75c946 (MIT)	0
2.5.2-75c946 (MIT)	0
2.6.2-75c946 ((Ruby OR (BSD-2-Clau...	0
2.8.0-75c946 (Apache 2.0)	0
3.2.5-75c946 (BSD-2-Clause)	0
6.1.6.1-75c946 (MIT)	0



OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

SBOM Mgmt

Choose project

Moya - 418d53

Search files...

Show all

Files

Overview

Inventory items

2.0.5-75c946 (MIT)

Inventory item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Filter

Resolved	ID	Aliases	Severity	Exploitability	Risk score
☐	VCD-Five-q3kw-aaak	CVE-2022-31163, GHSA-5cm2-98bc-rvfx	Medium	0.5	4

Update vulnerabilities

Create VEX

+ Create

Vulnerable X

Item

Files #

2.0.5-75c946 (MIT)

2.5.2-75c946 (MIT)

2.6.2-75c946 (Ruby OR (BSD-2-Clause...))

2.8.0-75c946 (Apache 2.0)

3.2.5-75c946 (BSD-2-Clause)

6.1.6.1-75c946 (MIT)

OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

Vulnerabilities

Choose project

Moya - 418d53

Filter

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
VCD-9mm-c5u9-hqe5	CVE-2026-32210, GHSA-3m6g-2423-7cp3	Medium	0.5	4	http://public.vulnerabilitycode.io/vulnerabilities/VCD-9mm-c5u9-hqe5	False	04/16/2026 10:03:39:082
VCD-yft-rs24-dftz	CVE-2025-56767, GHSA-c2t4-jgmc-q2t5	Low	0.5	2.4	http://public.vulnerabilitycode.io/vulnerabilities/VCD-yft-rs24-dftz	False	04/16/2026 10:31:56:624
VCD-ksaf-z7q3-groq	CVE-2026-25765, GHSA-33mb-2634-fwz2	Low	0.5	3.1	http://public.vulnerabilitycode.io/vulnerabilities/VCD-ksaf-z7q3-groq	False	04/16/2026 10:32:19:998
VCD-Ffive-q3kw-aaak	CVE-2022-31163, GHSA-5cm2-98bc-rvfx	Medium	0.5	4	http://public.vulnerabilitycode.io/vulnerabilities/VCD-Ffive-q3kw-aaak	False	04/16/2026 10:33:44:546
VCD-fnwi-akjy-aaah	CVE-2021-32740, GHSA-j4nc-q857-5jg	Medium	0.5	4	http://public.vulnerabilitycode.io/vulnerabilities/VCD-fnwi-akjy-aaah	False	04/16/2026 11:18:45:586
VCD-caw7-qjlk-aaas	CVE-2023-22796, GHSA-fgpc-792m-qgm2, GMS-2023-61	Low	0.5	3.4	http://public.vulnerabilitycode.io/vulnerabilities/VCD-caw7-qjlk-aaas	False	04/16/2026 11:26:45:755
VCD-eh4n-cqwc-aaah	CVE-2023-38037, GHSA-c15q-6q8f-rqlq	Low	0.5	3.1	http://public.vulnerabilitycode.io/vulnerabilities/VCD-eh4n-cqwc-aaah	False	04/16/2026 11:26:46:121
VCD-xpws-fy7b-aaq	CVE-2023-28120, GHSA-gj73-v5mw-pm9, GMS-2023-765	Low	0.5	3.1	http://public.vulnerabilitycode.io/vulnerabilities/VCD-xpws-fy7b-aaq	False	04/16/2026 11:26:49:745
VCD-6ul8-29nt-y7qe	CVE-2024-49761, GHSA-4xqp-v6pw-ch6m	Low	0.5	3.4	http://public.vulnerabilitycode.io/vulnerabilities/VCD-6ul8-29nt-y7qe	False	04/16/2026 11:26:50:063
VCD-9pk8-nxw6-aaad	CVE-2024-41123, GHSA-r55c-59qg-vjw6	Low	0.5	3.4	http://public.vulnerabilitycode.io/vulnerabilities/VCD-9pk8-nxw6-aaad	False	04/16/2026 11:26:50:405
VCD-gkvt-wgt2-aaan	CVE-2024-39908, GHSA-4xqp-v6pw-ch6m	Low	0.5	3.4	http://public.vulnerabilitycode.io/vulnerabilities/VCD-gkvt-wgt2-aaan	False	04/16/2026 11:26:50:758
VCD-muq7-stop-aaac	CVE-2024-35176, GHSA-vj3r-m7w-2zgh	Low	0.5	3.4	http://public.vulnerabilitycode.io/vulnerabilities/VCD-muq7-stop-aaac	False	04/16/2026 11:26:51:116
VCD-qk4e-4urp-5bwe	CVE-2024-43398, GHSA-vmwv-mc7x-5vc3	Medium	0.5	4	http://public.vulnerabilitycode.io/vulnerabilities/VCD-qk4e-4urp-5bwe	False	04/16/2026 11:26:51:479
VCD-qz3y-ratp-aaab	CVE-2024-41946, GHSA-5866-49q-22v4	Low	0.5	3.4	http://public.vulnerabilitycode.io/vulnerabilities/VCD-qz3y-ratp-aaab	False	04/16/2026 11:26:51:479

+ Create

Edit

Remove

Excel

JSON



OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

Software components

Choose project

Moya - 418d53

> Filter

Name

Version

PURL

Licenses

Curated

License controlled by AI

gh_inspector	1.1.3	pkg:gem/gh_inspector@1.1.3	MIT	False	
colored2	3.1.2	pkg:gem/colored2@3.1.2	MIT	False	
atomos	0.1.3	pkg:gem/atomos@0.1.3	MIT	False	
nap	1.1.0	pkg:gem/nap@1.1.0	MIT	False	
public_suffix	4.0.7	pkg:gem/public_suffix@4.0.7	MIT	False	
cocapods-plugins	1.0.0	pkg:gem/cocapods-plugins@1.0.0	MIT	False	
cocapods-trunk	1.6.0	pkg:gem/cocapods-trunk@1.6.0	MIT	False	
cocapods-search	1.0.1	pkg:gem/cocapods-search@1.0.1	MIT	False	
fuzzy_match	2.0.4	pkg:gem/fuzzy_match@2.0.4	MIT	False	
fourflusher	2.3.1	pkg:gem/fourflusher@2.3.1	MIT	False	
netrc	0.11.0	pkg:gem/netrc@0.11.0	MIT	False	
algoliasearch	1.27.5	pkg:gem/algoliasearch@1.27.5	MIT	False	
cocapods-deintegrate	1.0.5	pkg:gem/cocapods-deintegrate@1.0.5	MIT	False	
ruby-macho	2.5.1	pkg:gem/ruby-macho@2.5.1	MIT	False	
ruby2_keywords	0.0.5	pkg:gem/ruby2_keywords@0.0.5	Ruby, BSD-2-Clause	False	
mojibake	0.0.0	pkg:gem/mojibake@0.0.0	MIT	False	
escape	0.0.4	pkg:gem/escape@0.0.4	BSD-3-Clause	False	
cocapods-try	1.2.0	pkg:gem/cocapods-try@1.2.0	MIT	False	
addressable	2.8.0	pkg:gem/addressable@2.8.0	Apache-2.0	False	
rouge	2.0.7	pkg:gem/rouge@2.0.7	BSD-2-Clause, MIT	False	
zeitwerk	2.6.0	pkg:gem/zeitwerk@2.6.0	MIT	False	
faraday	2.5.2	pkg:gem/faraday@2.5.2	MIT	False	

+ Create

Edit

Remove

4.17.4.8 Promisekit

<https://github.com/mxcl/PromiseKit>

Vulnerabilities: 104

OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

Software components

Choose project

mxcl_PromiseKit - 2859

> Filter

Name

Version

PURL

Licenses

Curated

License controlled by AI

wrappy	1.0.2	pkg:npm/wrappy@1.0.2	ISC	False	
decamelize	1.2.0	pkg:npm/decamelize@1.2.0	MIT	False	
has-flag	3.0.0	pkg:npm/has-flag@3.0.0	MIT	False	
strip-json-comments	2.0.1	pkg:npm/strip-json-comments@2.0.1	MIT	False	
is-extendable	2.1.1	pkg:npm/is-extendable@2.1.1	MIT	False	
has-value	0.3.1	pkg:npm/has-value@0.3.1	MIT	False	
static-extend	0.1.2	pkg:npm/static-extend@0.1.2	MIT	False	
is-extendable	1.0.1	pkg:npm/is-extendable@1.0.1	MIT	False	
restore-cursor	1.0.1	pkg:npm/restore-cursor@1.0.1	MIT	False	
globby	4.1.0	pkg:npm/globby@4.1.0	MIT	False	
serialize-javascript	1.4.0	pkg:npm/serialize-javascript@1.4.0	BSD-3-Clause	False	
ansi-escapes	3.0.0	pkg:npm/ansi-escapes@3.0.0	MIT	False	
har-validator	4.2.1	pkg:npm/har-validator@4.2.1	ISC	False	
ssri	5.2.4	pkg:npm/ssri@5.2.4	ISC	False	
strip-eof	1.0.0	pkg:npm/strip-eof@1.0.0	MIT	False	
safe-regex	1.1.0	pkg:npm/safe-regex@1.1.0	MIT	False	
decompress-response	3.3.0	pkg:npm/decompress-response@3.3.0	MIT	False	
require-directory	2.1.1	pkg:npm/require-directory@2.1.1	MIT	False	
escape-string-regexp	1.0.5	pkg:npm/escape-string-regexp@1.0.5	MIT	False	
once	1.4.0	pkg:npm/once@1.4.0	ISC	False	
color-name	1.1.3	pkg:npm/color-name@1.1.3	MIT	False	
invariant	0.1.4	pkg:npm/invariant@0.1.4	MIT	False	

+ Create

Edit

Remove



Vulnerabilities									
Choose project									
mxcl_PromiseKit - 2859									
Filter									
1-100 rows of									
ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update		
VCD-23ze-v1m1-aaan	CVE-2022-33987, GHSA-pfrx-2q88-qg97	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VCD-23ze-v1m1-aaan	False	04/16/2026 10:01:48:637		
VCD-d1v1-pwv7-aaaa	GHSA-H6c3-v84p-w6p9, GMS-2019-21	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCD-d1v1-pwv7-aaaa	False	04/16/2026 11:34:42:731		
VCD-v5wp-2p9w-7bds	CVE-2025-54786, GHSA-6rwe-9888-hmc6	Low	0.5	1.4	http://public.vulnerablecode.io/vulnerabilities/VCD-v5wp-2p9w-7bds	False	04/16/2026 10:24:55:623		
VCD-7d2s-v291-47y4	CVE-2025-15284, GHSA-6rwe-9888-hmc6	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCD-7d2s-v291-47y4	False	04/16/2026 10:24:39:760		
VCD-vrmf-rgrv-f7az	CVE-2026-2391, GHSA-w7m-mew-8883	Low	0.5	2.9	http://public.vulnerablecode.io/vulnerabilities/VCD-vrmf-rgrv-f7az	False	04/16/2026 10:24:40:572		
VCD-qqa3-39f3-aaah	CVE-2023-28155, GHSA-p9s7-v289-3p64	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VCD-qqa3-39f3-aaah	False	04/16/2026 10:24:46:993		
VCD-exam-7f55-43av	CVE-2025-13465, GHSA-rxp-mmp-4qpy	Low	0.5	3.7	http://public.vulnerablecode.io/vulnerabilities/VCD-exam-7f55-43av	False	04/16/2026 10:25:37:021		
VCD-g9me-1erc-aaap	CVE-2024-4068, GHSA-gv7-rf6c-xmjp	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCD-g9me-1erc-aaap	False	04/16/2026 10:27:16:484		
VCD-bev-ry9-3aif	GHSA-5cd-j48t-rmmj	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCD-bev-ry9-3aif	False	04/16/2026 10:27:25:019		
VCD-caf7-a68-aaad	CVE-2023-28136, GHSA-72uf-gv4-eqf3	Medium	0.5	4.4	http://public.vulnerablecode.io/vulnerabilities/VCD-caf7-a68-aaad	False	04/16/2026 10:27:31:587		
VCD-nse1-pfv7-1ug7	CVE-2025-69873, GHSA-2p4f-4pww-qv6	Low	0.5	3.4	http://public.vulnerablecode.io/vulnerabilities/VCD-nse1-pfv7-1ug7	False	04/16/2026 10:27:49:897		
VCD-6m43-bellp-akey	CVE-2025-7785, GHSA-6p9-7rog-78p4	Medium	0.5	4.5	http://public.vulnerablecode.io/vulnerabilities/VCD-6m43-bellp-akey	False	04/16/2026 10:28:29:426		
VCD-p4b3-9uww-43g3	CVE-2026-27904, GHSA-23c5-xmqy-rm74	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCD-p4b3-9uww-43g3	False	04/16/2026 10:28:56:606		
VCD-rawd-zt1e-8tc3	CVE-2026-27903, GHSA-7f86-cg39-jmmj	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCD-rawd-zt1e-8tc3	False	04/16/2026 10:28:57:631		
VCD-v46t-afq4-qg9	CVE-2026-26996, GHSA-3poc-4f55-3m26	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCD-v46t-afq4-qg9	False	04/16/2026 10:28:57:662		
VCD-v6se-4mc2-fqpf	CVE-2025-5889, GHSA-66h2-p8h4-qcqw	Low	0.5	1.4	http://public.vulnerablecode.io/vulnerabilities/VCD-v6se-4mc2-fqpf	False	04/16/2026 10:28:16:649		
VCD-cw9m-7sf9-57m	CVE-2025-9288, GHSA-95m3-7q88-8ar5	Medium	0.5	4.5	http://public.vulnerablecode.io/vulnerabilities/VCD-cw9m-7sf9-57m	False	04/16/2026 10:28:49:634		
VCD-by7-fm1t-aaak	CVE-2022-0144, GHSA-4uq4-32zv-6wp6	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCD-by7-fm1t-aaak	False	04/16/2026 11:29:17:548		
VCD-np3k-ctf4-4ycu	CVE-2026-24001, GHSA-4uq4-32zv-6wp6	Low	0.5	3.4	http://public.vulnerablecode.io/vulnerabilities/VCD-np3k-ctf4-4ycu	False	04/16/2026 11:29:43:083		
VCD-9yfk-x533-aaad	GHSA-66h2-mmw6-vqhl, GMS-2022-11	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCD-9yfk-x533-aaad	False	04/16/2026 11:29:18:008		
VCD-tsbj-b8h4-aaaa	CVE-2019-16769, GHSA-hrv-jmef-4qpx	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCD-tsbj-b8h4-aaaa	False	04/16/2026 11:32:59:589		
VCD-hqhs-2qk7-aaam	CVE-2020-7660, GHSA-hacc-f52p-wc94	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCD-hqhs-2qk7-aaam	False	04/16/2026 11:32:59:241		
VCD-qc43-dnav-aaab	CVE-2021-27290, GHSA-vx3p-948g-6vqj	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCD-qc43-dnav-aaab	False	04/16/2026 11:33:02:788		
VCD-7mjh-3bae-aaaj	GHSA-6ctw-6fcp-f759, GMS-2020-702	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCD-7mjh-3bae-aaaj	False	04/16/2026 11:33:22:591		

SBOM Mgmt									
Choose project									
mxcl_PromiseKit - 2859									
Search files...									
Show all									
Files									
Overview									
Copyrights (0)									
Licenses (14)									
License	Number in software components								
BSD-2 Clause	18								
Artistic 2.0	1								
Unknown	2								
CC-BY 4.0	1								
MIT	634								
Unlicense	2								
CC0-1.0	3								
AFL 2.1	1								
Zlib	1								
Vulnerabilities (104)									

[illegible]



Octet Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

SBOM Mgmt

Choose project

mxcl_PromiseKit - 2859

Search files...

Show all

Files

Overview

Inventory items

4.0.1-2a4565 (MIT)

Inventory item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Filter

Resolved	ID	Aliases	Severity	Exploitability	Risk score
☐	VCD-8cua-12ba-egda	CVC-2024-43788, OHS-4rvj-4cpr-pf86	Low	0.5	3.1

Update vulnerabilities

Create VEX

+ Create

Vulnerable X

Item

Files #

0.0.29-d65779 (MIT)

0.0.33-9479ca (MIT)

0.0.8-46a89c (MIT)

0.1.0-a05d25 (MIT)

0.10.3-1301ba (MIT)

0.5.1-6e631c (MIT)

0.7.8-9e684b (BSD-3-Clause)

1.0.1-4d0884 (ISC)

1.0.0-99807 (MIT)

1.1.3-45a38f (MIT)

1.1.3-988807 (MIT)

of 4.0.0-f558ee (MIT)

1.13.0-381086 (MIT)

1.13.1-5af57b (MIT)

1.2.0-fe8997 (MIT)

1.3.4-3d9a68 (ISC)

1.3.5-241499 (ISC)

1.4.0-e28093 (BSD-3-Clause)

1.5.2-39c0db (MIT)

1.6.0-5d6e7d (MIT)

1.8.3-81169e (MIT)

1.9.2-3074c2 (MIT)

2.0.3-832b43 (MIT OR (MIT AND Apa..

2.16.3-e41a27 (BSD-3-Clause)

2.2.0-5a619a (MIT)

0.7.1-976119 (MIT)

2.2.1-480766 (ISC)

1.0.11-50891b (ISC)

4.17.4.9 Perfect

<https://github.com/PerfectlySoft/Perfect>

Vulnerabilities: 104



Octet Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

Vulnerabilities

Choose project
PerfectlySoft_Perfect -

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

+ Create

Edit

Remove

Excel

JSON

Octet Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

SBOM Mgmt

Choose project
PerfectlySoft_Perfect - 4c8349

Search files...

Show all

Files

Overview

Inventory items

Perfect-master-a60e65 (Apache-2.0)

Inventory Item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Inventory name

Perfect-master-a60e65 (Apache-2.0)

Parent inventory item

Software component

com.github.PerfectlySoft/Perfect

Download URL

git+https://github.com/PerfectlySoft/Perfect

Linking

Priority

Number of files

0

Curated

Created at: 04/16/2026 09:53:20:146

+ Create

Item

Files

Perfect-master-a60e65 (Apache-2.0)



4.17.4.10 Kitura

<https://github.com/Kitura/Kitura>

The screenshot displays the Occtet Curator SBOM Mgmt interface. The left sidebar contains a navigation menu with options: Dashboard, SBOM Mgmt, Vulnerabilities, VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and an Administration section with sub-items: Configuration, Organizations, Services, Users, and Backend logs. The main content area is titled 'SBOM Mgmt' and shows a project selection dropdown set to 'Kitura - 07e0ea'. Below this is a search bar and a 'Show all' button. The main view is divided into two tabs: 'Overview' and 'Inventory items'. The 'Overview' tab is active, showing a table with columns 'License' and 'Number in software components'. The table contains one entry: 'Apache 2.0' with a value of '1'. The 'Inventory items' tab is also visible, showing a table with columns 'Item' and 'Files #'. The 'Item' column contains 'Kitura-master-d6f8d2 (Apache 2.0)' and the 'Files #' column shows '0' with a warning icon. A '+ Create' button is located in the top right corner of the main content area. The bottom left corner shows the user 'admin' with a profile icon.



Occtet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration
 - Configuration
 - Organizations
 - Services
 - Users
 - Backend logs

SBOM Mgmt

Choose project
Kitura - 07e0ea

Search files...

Show all

Files

Overview
Inventory items

Kitura-master-d6f6b2 (Apache-2.0)

Inventory item
Vulnerabilities
Files
Audit notes
Licenses
Copyrights

Save

Item
Files

Kitura-master-d6f6b2 (Apache-2.0)

Inventory name
Kitura-master-d6f6b2 (Apache-2.0)

Parent inventory item
com.github.Kitura/Kitura

Download URL
git+https://github.com/Kitura/Kitura

Linking
Priority
Number of files
Curated

Created at: 04/16/2026 11:23:03:110

Occtet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration
 - Configuration
 - Organizations
 - Services
 - Users
 - Backend logs

Vulnerabilities

Choose project
Kitura - 07e0ea

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update

+ Create
Edit
Remove

Excel
JSON

OCCTET Deliverable Number: D 3.3 - SME Toolkit-Demo-Del - page 125

<https://github.com/davecgh/go-spew>

Octet Curator

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT Violation
Import
Help
Administration

[curator-admin]

SBOM Mgmt

Choose project
davecgh_go-spez - 1.1.1

Search files...
Show all

Files 0

Overview Inventory Items

go-spez-master-0b279a (ISC)

Inventory Item
Vulnerabilities
Files
Audit notes
Licenses
Copyrights

Save

Inventory name

go-spez-master-0b279a (ISC)

Parent inventory item

com.github.davecgh/go-spez

com.github.davecgh/go-spez

Download URL

git+https://github.com/davecgh/go-spez

Download

Linking

Priority

Number of files

0

Curated

Created at: 04/16/2026 13:36:30:457

Create

Item 0
Files 0

go-spez-master-0b279a (ISC)



Octet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities**
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration

Vulnerabilities

Choose project
daveagh_go-spew - 1.1

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

[curator-admin] [Create] [Edit] [Remove] [Excel] [JSON]

4.17.5.3 Go-yaml-3.0.1

<https://github.com/go-yaml/yaml/tree/v3.0.1>

Octet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities**
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration

SBOM Mgmt

Choose project
go-yaml - 3.0.1

Search files... Show all

Files
yaml

Inventory Items

yaml-yaml-v3-8b5457 (NOASSERTION)

Parent inventory item
Software component
com.github.go-yaml.yaml

Download URL
git+https://github.com/go-yaml/yaml

Linking
Priority
Number of files
0
Curated

Created at: 04/16/2026 13:32:49:578

[curator-admin] [Create] [Save] [Item] [Files]



Occtet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities**
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration

Vulnerabilities

Choose project
go-yaml - 3.0.1

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

[Create] [Edit] [Remove]

[Export] [JSON]

4.17.5.4 Modern-go-concurrent

<https://github.com/modern-go/concurrent>

Occtet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities**
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration

SBOM Mgmt

Choose project
modern-go-concurrent - 0.0.0-20180

Search files...
Show all

Files

Overview

Inventory Items

go-concurrent-master-31dbct (Apache-2.0)

Inventory Item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Item

Files

go-concurrent-master-31dbct (Apache-2.0)

Inventory name
go-concurrent-master-31dbct (Apache-2.0)

Parent inventory item

Software component

com.github.modern-go/concurrent

Download URL
git+https://github.com/modern-go/concurrent

Linking

Priority

Number of files

0

Curated

Created at: 04/16/2026 13:53:00:015

4.17.5.5 Modern-go-reflect2

<https://github.com/modern-go/reflect2>

Acetec Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

[admin]

SBOM Mgmt

Choose project

modern-go_reflect2 - 1.0.2

Search files...

Show all

Files 0

Overview

Inventory items

go-reflect2-master-97d0fc (Apache 2.0)

Inventory Item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Inventory name

go-reflect2-master-97d0fc (Apache 2.0)

Parent inventory item

Software component

com.github.modern-go/reflect2

Download URL

git+https://github.com/modern-go/reflect2

Linking

Priority

Number of files

0

Curated

Created at: 04/16/2026 14:03:08:970

+ Create

Item 0

Files 0

go-reflect2-master-97d0fc (Apache 2.0)



4.17.5.6 Pflag-1.0.5

<https://github.com/spf13/pflag>

4.17.5.7 Pmezard-go-difflib

<https://github.com/pmezard/go-difflib>



Octet Curator SBOM Mgmt

Choose project: pmezard_go-diffib - 1.0.0

Search files... 0/0

Show all

Files 0

Inventory name: go-diffib-master-332f43 (NOASSERTION)

Parent inventory item: com.github.pmezard/go-diffib

Software component: com.github.pmezard/go-diffib

Download URL: git+https://github.com/pmezard/go-diffib

Linking: Priority: Number of files: 0 Curated

Created at: 04/16/2026 13:33:48:200

Octet Curator Vulnerabilities

Choose project: pmezard_go-diffib - 1.0.0

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update

Created at: 04/16/2026 13:33:48:200

Buttons: Create, Edit, Remove, Excel, JSON

4.17.5.8 Stretchr_testify

<https://github.com/stretchr/testify>



OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

[admin]

SBOM Mgmt

Choose project
stretchr_testify - 1.10.0

Search files...
Show all

Files

Overview

Inventory items

action-gh-release-2..75c9462.*.* (NOASSERTION)

Inventory item

Parent inventory item
testify-master-038a44 (MIT)

Software component
soffprops/action-gh-release

Download URL
NOASSERTION

Linking

Priority

Number of files
0

Curated

Created at: 04/16/2026 13:53:26:288

+ Create

Item

Files

testify-master-038a44 (MIT)

action-gh-release-2..75c9462.*.* (NO...

checkout-5..75c9462.*.* (NOASSERTI...

jinenez-popen-0.0.0-201801252023...

cdpi-0.5.2-75c946 (MIT)

setup-go-6..75c9462.*.* (NOASSERTI...

yamll.v3.0.1-75c946 (Apache 2.0)

OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

[admin]

Vulnerabilities

Choose project
stretchr_testify - 1.10.0

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

+ Create Edit Remove

Excel JSON



4.17.5.9 Text-0.21.0

<https://cs.opensource.google/go/x/text>

The screenshot shows the 'Occtet Curator' application interface. The left sidebar contains navigation links: Dashboard, SBOM Mgmt, Vulnerabilities, VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and Administration. The main area is titled 'SBOM Mgmt' and shows a list of projects. The selected project is 'go-text - 0.21.0'. The 'Inventory items' tab is active, displaying a table with columns: Inventory name, Parent inventory item, Software component, Download URL, Linking, Priority, Number of files, and Curated. The table contains one item: 'module-golang.org-x-mod-5ef6046c70b2c760v0.17.0 (NOASSERTION)'. The 'Download URL' is 'NOASSERTION'. The 'Linking' dropdown is set to 'Linking'. The 'Priority' is 'Priority'. The 'Number of files' is '0'. The 'Curated' checkbox is checked. The 'Created at' timestamp is '04/23/2026 14:35:00:185'.

The screenshot shows the 'Occtet Curator' application interface. The left sidebar contains navigation links: Dashboard, SBOM Mgmt, Vulnerabilities, VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and Administration. The main area is titled 'Vulnerabilities' and shows a table with columns: ID, Aliases, Severity, Exploitability, Risk score, Source URL, Manually created, and Last update. The table is empty. The 'Create' button is visible at the bottom left, and the 'Excel' and 'JSON' buttons are visible at the bottom right.



4.17.5.10 Yaml-2.4.0

<https://github.com/go-yaml/yaml>

The screenshot displays the Occtet Curator web application interface. The left sidebar contains a navigation menu with options: Dashboard, SBOM Mgmt, Vulnerabilities, VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and Administration. The main content area is divided into two sections.

SBOM Mgmt Section:

- Choose project:** go-yaml_yaml - 2.4.0
- Search files:** Search files... (with a dropdown for 0/0)
- Show all:** A button to view all files.
- Files:** A list showing a file named 'yaml'.
- Overview / Inventory items:**
 - Inventory name:** yaml-yaml-v3-8b5457 (NOASSERTION)
 - Parent inventory item:** A dropdown menu.
 - Software component:** com.github.go-yaml.yaml
 - Download URL:** git+https://github.com/go-yaml/yaml
 - Linking:** A dropdown menu.
 - Priority:** A dropdown menu.
 - Number of files:** 0
 - Curated:** A checkbox.
- Created at:** 04/16/2026 13:51:332

Vulnerabilities Section:

- Choose project:** go-yaml_yaml - 2.4.0
- Table headers:** ID, Aliases, Severity, Exploitability, Risk score, Source URL, Manually created, Last update.
- Table content:** The table is currently empty.
- Actions:** + Create, Edit, Remove buttons at the bottom.
- Export:** Excel, JSON buttons at the bottom right.



4.17.6 Ruby Projects

4.17.6.1 Rails

<https://github.com/rails/rails>

Octet Curator

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT Issues
ORT Violation
Import
Help
Administration
Configuration
Organizations
Services
Users
Backend logs

[admin]

Software components

Choose project

Rails - 4c0f7952

> Filter

1-100 rows of

Name	Version	PURL	Licenses	Curated	License controlled by AI
destroy	1.2.0	pkg:rpm/destroy@1.2.0	MIT	False	
graceful-fs	4.2.11	pkg:rpm/graceful-fs@4.2.11	ISC	False	
has-flag	4.0.0	pkg:rpm/has-flag@4.0.0	MIT	False	
toidentifier	1.0.1	pkg:rpm/toidentifier@1.0.1	MIT	False	
setprototypeof	1.2.0	pkg:rpm/setprototypeof@1.2.0	ISC	False	
debug	4.3.4	pkg:rpm/debug@4.3.4	MIT	False	
wrappy	1.0.2	pkg:rpm/wrappy@1.0.2	ISC	False	
connect	3.7.0	pkg:rpm/connect@3.7.0	MIT	False	
color-convert	1.9.3	pkg:rpm/color-convert@1.9.3	MIT	False	
get-caller-file	2.0.5	pkg:rpm/get-caller-file@2.0.5	ISC	False	
range-parser	1.2.1	pkg:rpm/range-parser@1.2.1	MIT	False	
escape-html	1.0.3	pkg:rpm/escape-html@1.0.3	MIT	False	
strip-ansi	6.0.1	pkg:rpm/strip-ansi@6.0.1	MIT	False	
depd	2.0.0	pkg:rpm/depd@2.0.0	MIT	False	
has-flag	3.0.0	pkg:rpm/has-flag@3.0.0	MIT	False	
encodeurl	1.0.2	pkg:rpm/encodeurl@1.0.2	MIT	False	
is-extendable	2.1.1	pkg:rpm/is-extendable@2.1.1	MIT	False	
minimist	1.2.8	pkg:rpm/minimist@1.2.8	MIT	False	
universalify	0.1.2	pkg:rpm/universalify@0.1.2	MIT	False	
ee-first	1.1.1	pkg:rpm/ee-first@1.1.1	MIT	False	
on-finished	2.3.0	pkg:rpm/on-finished@2.3.0	MIT	False	
unpipe	1.0.0	pkg:rpm/unpipe@1.0.0	MIT	False	

+ Create
Edit
Remove

Octet Curator

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT Issues
ORT Violation
Import
Help
Administration
Configuration
Organizations
Services
Users
Backend logs

[admin]

Vulnerabilities

Choose project

Rails - 4c0f7952

> Filter

21 rows

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
VDID-ekjp-1e1g-aaas	CVE-2021-3807, GHSA-93q8-gg69-wqmw	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDID-ekjp-1e1g-aaas	False	04/16/2026 10:03:14.510
VDID-v5wg-2p1w-70ds	CVE-2025-54788, GHSA-5215-8888-hmcs	Low	0.5	1.4	http://public.vulnerablecode.io/vulnerabilities/VDID-v5wg-2p1w-70ds	False	04/16/2026 10:24:55.623
VDID-7x2s-s214-67g4	CVE-2025-15284, GHSA-6nw7-rpzm-49lp	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDID-7x2s-s214-67g4	False	04/16/2026 10:24:39.760
VDID-tzvg-nmkc-aaan	CVE-2022-34999, GHSA-rp9p-h999-3jpp	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDID-tzvg-nmkc-aaan	False	04/16/2026 10:24:40.159
VDID-vnmf-rqsr-17az	CVE-2026-2391, GHSA-w7fw-njwx-w883	Low	0.5	2.9	http://public.vulnerablecode.io/vulnerabilities/VDID-vnmf-rqsr-17az	False	04/16/2026 10:24:40.572
VDID-nqa2-39f3-aaah	CVE-2023-28155, GHSA-p8p7-e288-28g6	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDID-nqa2-39f3-aaah	False	04/16/2026 10:24:46.893
VDID-3mt-2upp-cdgr	CVE-2025-21610, GHSA-j863-3444-qpwj	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDID-3mt-2upp-cdgr	False	04/16/2026 10:25:08.481
VDID-7cgt-ttze-aaae	CVE-2024-43368, GHSA-gm2c-9f3c-2vcv	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDID-7cgt-ttze-aaae	False	04/16/2026 10:25:08.862
VDID-9rap-huzh-77b4	CVE-2025-46812, GHSA-mc2w-746g-9dth	Low	0.5	1.4	http://public.vulnerablecode.io/vulnerabilities/VDID-9rap-huzh-77b4	False	04/16/2026 10:25:09.235
VDID-cusb-cyfh-nuhg	GHSA-g8fg-w8rm-g96v	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDID-cusb-cyfh-nuhg	False	04/16/2026 10:25:09.626
VDID-w3kp-t5f3-aaas	CVE-2024-34341, GHSA-gpwp-rf96-cf99	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDID-w3kp-t5f3-aaas	False	04/16/2026 10:25:10.022
VDID-2k8s-g8f8-rcb8	CVE-2024-53847, GHSA-6vx4-q2w-qmgh	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDID-2k8s-g8f8-rcb8	False	04/16/2026 10:25:10.388
VDID-eeam-7f55-43ev	CVE-2025-13465, GHSA-nxj-mmjv-4ppg	Low	0.5	3.7	http://public.vulnerablecode.io/vulnerabilities/VDID-eeam-7f55-43ev	False	04/16/2026 10:25:37.021
VDID-1tkk-cxpb-aaac	CVE-2022-0613, GHSA-gc8f-g84f-25x5	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDID-1tkk-cxpb-aaac	False	04/16/2026 10:25:43.723
VDID-9k62-8t8b-aaan	CVE-2022-1233, GHSA-g694-m8vq-gv9h	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDID-9k62-8t8b-aaan	False	04/16/2026 10:25:44.103
VDID-ba1j-ye7s-aaar	CVE-2021-3647, GHSA-89gv-h8wf-cdfr	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDID-ba1j-ye7s-aaar	False	04/16/2026 10:25:44.896
VDID-es2v-clgn-aaam	CVE-2021-27516, GHSA-p69p-7zbc-rhwp	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDID-es2v-clgn-aaam	False	04/16/2026 10:25:45.927
VDID-k75h-jtgg-aaag	CVE-2020-26291, GHSA-3229-g8vv-fpgp	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDID-k75h-jtgg-aaag	False	04/16/2026 10:25:45.927
VDID-f5uv-86mk-aaaa	CVE-2022-1243, GHSA-3vf-827f-p6d3	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDID-f5uv-86mk-aaaa	False	04/16/2026 10:25:46.022
VDID-vu5f-q4ty-aaah	CVE-2022-24723, GHSA-gm4f-4438-p67f	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VDID-vu5f-q4ty-aaah	False	04/16/2026 10:25:46.027
VDID-wcef-hfnd-aaag	CVE-2022-0864, GHSA-8h2f-7c2f-7m3m	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VDID-wcef-hfnd-aaag	False	04/16/2026 10:25:46.477

+ Create
Edit
Remove

Excel
JSON



SBOM Mgmt

Choose project

Rails - 4c07952

Search files...

Show all

Files

[admin]

Overview

Inventory items

Copyrights (0)

Licenses (23)

Vulnerabilities (21)

License	Number in software components
BSD-2-Clause	42
GPL 3.0 or later	1
CC-BY-NC-SA 4.0	1
QPL 1.1	2
LOPL 2.1 only	1
APL 3.0	1
Unknown	4
MIT	533
Unlicense	2

+ Create

Item

Files #

rails-main-761819 (MIT)

0.0.20-75c946 (MIT)

0.0.5-75c946 ((BSD-2-Clause OR ...

0.1.0-75c946 (MIT)

0.1.0-75c946 (Unlicense)

0.1.16-75c946 (MIT)

0.12.0-75c946 (MIT)

0.16.11-75c946 (MIT)

0.19.0-75c946 (Apache-2.0)

0.2.0-75c946 ((BSD-2-Clause A...

0.2.0-75c946 (MIT)

0.2.2-75c946 (Apache-2.0)

0.2.27-75c946 (MIT)

0.2.5-75c946 (MIT AND Apache...

0.2.6-75c946 (MIT)

0.3.0-75c946 ((BSD-2-Clause A...

0.3.0-75c946 (NOASSERTION)

0.4.1-75c946 ((BSD-2-Clause OR ...

0.4.2-75c946 ((BSD-2-Clause OR ...

0.4.3-75c946 ((BSD-2-Clause A...

0.4.6-75c946 (MIT)

0.5.6-75c946 (MIT)

0.6.1-75c946 ((BSD-2-Clause A...

0.6.1-75c946 ((BSD-2-Clause AN...

0.6.2-75c946 ((BSD-2-Clause A...

0.8.1-75c946 (MIT)

1.0.0-75c946 (MIT)

1.0.3-75c946 ((BSD-2-Clause A...

SBOM Mgmt

Choose project

Rails - 4c07952

Search files...

Show all

Files

[admin]

Overview

Inventory items

Copyrights (0)

Licenses (23)

Vulnerabilities (21)

Vulnerability	Risk score of vulnerability	Number in software components
VCID-k75h-jdpg-aaag	4	1
VCID-es2v-clgn-aaam	4	1
VCID-exam-7s55-43ev	3.7	1
VCID-wzef-h6ad-aaag	4	1
VCID-91ap-hu2h-77b4	1.4	1
VCID-ekjb-telg-aaas	4	1
VCID-7cgt-tnez-aaae	3.1	1
VCID-cusb-cyfh-euqg	3.1	1
VCID-tpa2-39d3-aaah	3.1	1

+ Create

Item

Files #

rails-main-761819 (MIT)

0.0.20-75c946 (MIT)

0.0.5-75c946 ((BSD-2-Clause OR ...

0.1.0-75c946 (MIT)

0.1.0-75c946 (Unlicense)

0.1.16-75c946 (MIT)

0.12.0-75c946 (MIT)

0.16.11-75c946 (MIT)

0.19.0-75c946 (Apache-2.0)

0.2.0-75c946 ((BSD-2-Clause A...

0.2.0-75c946 (MIT)

0.2.2-75c946 (Apache-2.0)

0.2.27-75c946 (MIT)

0.2.5-75c946 (MIT AND Apache...

0.2.6-75c946 (MIT)

0.3.0-75c946 ((BSD-2-Clause A...

0.3.0-75c946 (NOASSERTION)

0.4.1-75c946 ((BSD-2-Clause OR ...

0.4.2-75c946 ((BSD-2-Clause OR ...

0.4.3-75c946 ((BSD-2-Clause A...

0.4.6-75c946 (MIT)

0.5.6-75c946 (MIT)

0.6.1-75c946 ((BSD-2-Clause A...

0.6.1-75c946 ((BSD-2-Clause AN...

0.6.2-75c946 ((BSD-2-Clause A...

0.8.1-75c946 (MIT)

1.0.0-75c946 (MIT)

1.0.3-75c946 ((BSD-2-Clause A...



OCCTET Curator

SBOM Mgmt

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

Choose project

Rails - 4c0f7952

Search files...

Show all

Files

Overview

Inventory items

1.17.1-94fad0 (MIT)

Inventory item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Inventory name

1.17.1-94fad0 (MIT)

Parent inventory item

socket-2.0.0-bb47c2 (MIT)

Software component

urijs

Download URL

NOASSERTION

Linking

Priority

Number of files

0

Curated

Created at: 04/16/2026 10:23:25:626

+ Create

Vulnerable X

Item

Files #

0.2.3-171123 (MIT)

0

0 A 0

1.17.1-94fad0 (MIT)

1

0 A 0

2.0.5-c0405d (MIT)

0

0 A 0

2.88.0-58e639 (Apache 2.0)

0

0 A 0

3.0.2-842536 (MIT)

0

0 A 0

4.17.21-bdb9f1 (MIT AND CC0-1.0)

0

0 A 0

6.11.0-e9f449 (BSD-3-Clause)

0

0 A 0

6.12.6-746cx3 (MIT)

0

0 A 0

javascript:4.0.0-1b8bdf (BSD-3-Clause)

0

0 A 0

redirects:1.15.2-23334c (MIT)

0

0 A 0

reggie:5.0.1-c0393f (MIT)

0

0 A 0

OCCTET Curator

SBOM Mgmt

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

Choose project

Rails - 4c0f7952

Search files...

Show all

Files

Overview

Inventory items

1.17.1-94fad0 (MIT)

Inventory item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Filter

8 rows

Resolved	ID	Aliases	Severity	Exploitability	Risk score
☐	VCD-vut5-q4ey-aaah	CVE-2022-24723, GHSA-gm44-4338-p67f	Low	0.5	3.1
☐	VCD-rhgv-Blenk-aaaa	CVE-2022-1243, GHSA-3yfl-82ff-p4r3	Medium	0.5	4
☐	VCD-ba1yq7s-aaar	CVE-2021-3647, GHSA-89gq-hblwf-cgfr	Low	0.5	3.1
☐	VCD-wzrf-hdod-aaqj	CVE-2022-0868, GHSA-Bh2f-7yc4-7m3m	Medium	0.5	4
☐	VCD-7ink-cxpb-aaac	CVE-2022-0613, GHSA-gcr8-gh4e-25e8	Medium	0.5	4
☐	VCD-Rk52-Bvel-aaan	CVE-2022-1233, GHSA-g694-m8hg-grHh	Medium	0.5	4
☐	VCD-475h-jqtp-aaqj	CVE-2020-26291, GHSA-3329-jjwv-fsqj	Medium	0.5	4
☐	VCD-ex2v-clgn-aaan	CVE-2021-27516, GHSA-pl6f-7htc-rhwg	Medium	0.5	4

Update vulnerabilities

Create VEX

+ Create

Vulnerable X

Item

Files #

0.2.3-171123 (MIT)

0

0 A 0

1.17.1-94fad0 (MIT)

1

0 A 0

2.0.5-c0405d (MIT)

0

0 A 0

2.88.0-58e639 (Apache 2.0)

0

0 A 0

3.0.2-842536 (MIT)

0

0 A 0

4.17.21-bdb9f1 (MIT AND CC0-1.0)

0

0 A 0

6.11.0-e9f449 (BSD-3-Clause)

0

0 A 0

6.12.6-746cx3 (MIT)

0

0 A 0

javascript:4.0.0-1b8bdf (BSD-3-Clause)

0

0 A 0

redirects:1.15.2-23334c (MIT)

0

0 A 0

reggie:5.0.1-c0393f (MIT)

0

0 A 0



4.17.6.2 Nokogiri

<https://github.com/sparklemotion/nokogiri>

Occtet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities**
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration
 - Configuration
 - Organizations
 - Services
 - Users
 - Backend logs

Vulnerabilities

Choose project

tion_Nokogiri - 39124

> Filter

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
VCD-17wu-7efc-aaae	CVE-2018-100544, GHSA-vgqg-mmwe-mcng	Medium	0.5	4.5	http://public.vulnerabilitycode.io/vulnerabilities/VCD-17wu-7efc-aaae	False	04/16/2026 10:55:42:887
VCD-q811-map7-aaas	CVE-2019-16892, GHSA-5m2v-hc54-56m6	Low	0.5	3.2	http://public.vulnerabilitycode.io/vulnerabilities/VCD-q811-map7-aaas	False	04/16/2026 10:55:43:251
VCD-g9ww-vu14-aaad	CVE-2017-5944, GHSA-gqqc-wfqp-n9p9	Medium	0.5	4.5	http://public.vulnerabilitycode.io/vulnerabilities/VCD-g9ww-vu14-aaad	False	04/16/2026 10:55:43:674
VCD-vys5-nb11-aaad	GHSA-3q5c-179q-7br2	Medium	0.5	4.4	http://public.vulnerabilitycode.io/vulnerabilities/VCD-vys5-nb11-aaad	False	04/16/2026 10:55:44:107

[admin] [Create] [Edit] [Remove] [Excel] [JSON]

Occtet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities
- VEX listing
- Projects
- Software components**
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration
 - Configuration
 - Organizations
 - Services
 - Users
 - Backend logs

Software components

Choose project

tion_Nokogiri - 39124

> Filter

Name	Version	PURL	Licenses	Curated	License controlled by AI
ruby/setup-ruby	1.**	pkg:githubactions/ruby/setup-ruby@1.%2A.%2A		False	
actions/checkout	6.**	pkg:githubactions/actions/checkout@6.%2A.%2A		False	
ruby/setup-ruby-pkgs	1.**	pkg:githubactions/ruby/setup-ruby-pkgs@1.%2A.%2A		False	
rubocop-packaging	0.6.0	pkg:gem/rubocop-packaging@0.6.0	MIT	False	
rake	13.3.0	pkg:gem/rake@13.3.0	Unknown, MIT	False	
minitest-mock	5.27.0	pkg:gem/minitest-mock@5.27.0	MIT	False	
rescical	1.0.8	pkg:gem/rescical@1.0.8	LOPL-2.1-only	False	
ruby_memcheck	3.0.1	pkg:gem/ruby_memcheck@3.0.1	MIT	False	
standard	1.50.0	pkg:gem/standard@1.50.0	MIT	False	
rubocop-minitest	0.38.2	pkg:gem/rubocop-minitest@0.38.2	MIT	False	
rubyrtp	--> 3.1.0	pkg:gem/rubyrtp		False	
rake-compiler-dock	1.11.1	pkg:gem/rake-compiler-dock@1.11.1	MIT	False	
minitest-parallel_fork	2.1.1	pkg:gem/minitest-parallel_fork@2.1.1	MIT	False	
rubocop-rake	0.7.1	pkg:gem/rubocop-rake@0.7.1	MIT	False	
rake-compiler	1.3.1	pkg:gem/rake-compiler@1.3.1	MIT	False	
minitest	6.0.1	pkg:gem/minitest@6.0.1	MIT	False	
simplecov	0.22.0	pkg:gem/simplecov@0.22.0	MIT	False	
mini_portile2	--> 2.8.2	pkg:gem/mini_portile2		False	
racc	--> 1.4	pkg:gem/racc		False	
ruby/setup-ruby	d3c3b0d32a2222a8ac878b0c7daba78864e134	pkg:githubactions/ruby/setup-ruby@d3c3b0d32a2222a8ac878b0c7daba78864e134		False	
actions/cache	4.**	pkg:githubactions/actions/cache@4.%2A.%2A		False	
vmactions/freebsd-vm	1.**	pkg:githubactions/vmactions/freebsd-vm@1.%2A.%2A		False	

[admin] [Create] [Edit] [Remove]

OCCTET Deliverable Number: D 3.3 - SME Toolkit-Demo-Del - page 138



SBOM Mgmt

Choose project

Spraklemotion_Nokogiri - 39124

Search files...

Show all

Files

Overview

Inventory items

> Copyrights (0)

> Licenses (3)

License	Number in software components
MIT	13
LOPL 2.1 only	1
Unknown	1

> Vulnerabilities (4)

+ Create

Item	Files #
nokogiri-main-b6be39 (MIT)	0
0.22.0-75c946 (MIT)	0
1.0.8-75c946 (LOPL 2.1 only)	0
1.50.0-75c946 (MIT)	0
13.3.0-75c946 (MIT AND Licens...	0
3.0.1-75c946 (MIT)	0
6.0.1-75c946 (MIT)	0
75c946-- 1.4 (NOASSERTION)	0
75c946-- 2.8.2 (NOASSERTION)	0
75c946-- 3.1.0 (NOASSERTION)	0
build-push-action-7-75c9467 *...	0
cache-4-75c9464 ** (NOASSE...	0
checkout-6-75c9466 ** (NOAS...	0
compiler-1.3.1-75c946 (MIT)	0
compiler-dock-1.11.1-75c946 (M...	0
download-artifact-8-75c9468 *...	0
freedownload-vms-1-75c9461 ** (NO...	0
install-nix-action-31-75c94631...	0
login-action-4-75c9464 ** (NO...	0
minitest-0.38.2-75c946 (MIT)	0
mock-5.27.0-75c946 (MIT)	0
packaging-0.6.0-75c946 (MIT)	0
parallelfork-2.1.1-75c946 (MIT)	0
rake-0.7.1-75c946 (MIT)	0
setup-build-action-4-75c9464...	0
setup-java-5-75c9465 ** (NOA...	0
setup-ruby-1-75c9461 ** (NOA...	0
setup-ruby-43e3b032ad2222a8...	0

SBOM Mgmt

Choose project

Spraklemotion_Nokogiri - 39124

Search files...

Show all

Files

Overview

Inventory items

> Copyrights (0)

> Licenses (3)

> Vulnerabilities (4)

Vulnerability	Risk score of vulnerability	Number in software components
VCD-17wo-76c-aaae	4.5	1
VCD-a81-map7-aas	3.2	1
VCD-qhww-vq14-aaad	4.5	1
VCD-vyn5-n81-aaad	4.4	1

+ Create

Item	Files #
nokogiri-main-b6be39 (MIT)	0
0.22.0-75c946 (MIT)	0
1.0.8-75c946 (LOPL 2.1 only)	0
1.50.0-75c946 (MIT)	0
13.3.0-75c946 (MIT AND Licens...	0
3.0.1-75c946 (MIT)	0
6.0.1-75c946 (MIT)	0
75c946-- 1.4 (NOASSERTION)	0
75c946-- 2.8.2 (NOASSERTION)	0
75c946-- 3.1.0 (NOASSERTION)	0
build-push-action-7-75c9467 *...	0
cache-4-75c9464 ** (NOASSE...	0
checkout-6-75c9466 ** (NOAS...	0
compiler-1.3.1-75c946 (MIT)	0
compiler-dock-1.11.1-75c946 (M...	0
download-artifact-8-75c9468 *...	0
freedownload-vms-1-75c9461 ** (NO...	0
install-nix-action-31-75c94631...	0
login-action-4-75c9464 ** (NO...	0
minitest-0.38.2-75c946 (MIT)	0
mock-5.27.0-75c946 (MIT)	0
packaging-0.6.0-75c946 (MIT)	0
parallelfork-2.1.1-75c946 (MIT)	0
rake-0.7.1-75c946 (MIT)	0
setup-build-action-4-75c9464...	0
setup-java-5-75c9465 ** (NOA...	0
setup-ruby-1-75c9461 ** (NOA...	0
setup-ruby-43e3b032ad2222a8...	0



Occtet Curator

SBOM Mgmt

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT Issues
ORT Violation
Import
Help
Administration
Configuration
Organizations
Services
Users
Backend logs

Choose project
Spraklemotion_Nokogiri - 391244

Search files...

Show all

Files

Overview
Inventory items

75c946--> 3.1.0 (NOASSERTION)

Inventory item
Vulnerabilities
Files
Audit notes
Licenses
Copyrights

Save

Inventory name
75c946--> 3.1.0 (NOASSERTION)

Parent inventory item
nokogiri-main-b6be39 (MIT)

Software component
rubyzip

Download URL
NOASSERTION

Linking
Priority
Number of files
0

Curated

Created at: 04/16/2026 10:55:35:256

+ Create

Vulnerable X

Item
Files

75c946--> 3.1.0 (NOASSERTION)

Occtet Curator

SBOM Mgmt

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT Issues
ORT Violation
Import
Help
Administration
Configuration
Organizations
Services
Users
Backend logs

Choose project
Spraklemotion_Nokogiri - 391244

Search files...

Show all

Files

Overview
Inventory items

75c946--> 3.1.0 (NOASSERTION)

Inventory item
Vulnerabilities
Files
Audit notes
Licenses
Copyrights

Save

> Filter

Resolved	ID	Aliases	Severity	Exploitability	Risk score
	VCID-gfhw-vul4-aaad	CVE-2017-5946, GHSA-ggqj-wfgr-1909	Medium	0.5	4.5
	VCID-gym5-nbt1-aaad	GHSA-3q5q-r79q-7hr2	Medium	0.5	4.4
	VCID-qlt1-mmp7-aass	CVE-2019-16892, GHSA-5m2v-hc64-56h6	Low	0.5	3.2
	VCID-17w9-7f6c-aaae	CVE-2018-1000544, GHSA-rqcg-nrmw-ncmg	Medium	0.5	4.5

4 ROWS

Update vulnerabilities
Create VEX

+ Create

Vulnerable X

Item
Files

75c946--> 3.1.0 (NOASSERTION)



4.17.6.3 Ruby/JSON

<https://github.com/ruby/json>

Octet Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

Software components

Choose project

Ruby_Json - 3946e5

> Filter

Name	Version	PURL	Licenses	Curated	License controlled by AI
actions/checkout	6.**	pkg.githubactions/actions/checkout@6.%2A.%2A		False	
ruby/setup-ruby-pkgs	1.**	pkg.githubactions/ruby/setup-ruby-pkg@1.%2A.%2A		False	
benchmark-ips	>= 0	pkg.gem/benchmark-ips		False	
rapidjson	>= 0	pkg.gem/rapidjson		False	
power_assert	< 3.0.0	pkg.gem/power_assert		False	
net-http	>= 0	pkg.gem/net-http		False	
rake-compiler	>= 0	pkg.gem/rake-compiler		False	
test-unit	>= 0	pkg.gem/test-unit		False	
test-unit-ruby-core	>= 0	pkg.gem/test-unit-ruby-core		False	
ruby/actions/ github/workflows/ruby_versions.yml	master	pkg.githubactions/ruby/actions/ github/workflows/rub_...		False	
correctional/triggers-workflow-and-wait	1.6.5	pkg.githubactions/correctional/triggers-workflow-and-w...		False	
actions/create-github-app-token	3.**	pkg.githubactions/actions/create-github-app-token@3...		False	
com.github.ruby/json	master	pkg.github/ruby/json@master		False	

+ Create

Edit

Remove

[admin]

Octet Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

Vulnerabilities

Choose project

Ruby_Json - 3946e5

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

+ Create

Edit

Remove

[admin]

Excel

JSON



OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

SBOM Mgmt

Choose project

Ruby_json - 3946e5

Search files...

Show all

Files

Overview

> Copyrights (0)

> Licenses (0)

> Vulnerabilities (0)

+ Create

Item

Files #

json-master-3fe18 (NOASSERTION)

0

75c946-3.0.0 (NOASSERTION)

0

75c946-0 (NOASSERTION)

0

checkout-6..75c946.*.* (NOAS..)

0

compiler-75c946-0 (NOASSER..)

0

create-github-app-token-3..75c9..

0

http-75c946-0 (NOASSERTION)

0

ip-75c946-0 (NOASSERTION)

0

rubyversions.yml-master-75c946..

0

setup-ruby-plugs-1..75c9461.*.*

0

trigger-workflow-and-wait-1.6.5..

0

unit-75c946-0 (NOASSERTION)

0

unit-ruby-core-75c946-0 (NOA..)

0

OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

SBOM Mgmt

Choose project

Ruby_json - 3946e5

Search files...

Show all

Files

Overview

Inventory items

75c946-0 (NOASSERTION)

Inventory item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Inventory name

75c946-0 (NOASSERTION)

Parent inventory item

json-master-3fe18 (NOASSERTION)

Software component

rapidjson

Download URL

NOASSERTION

Linking

Priority

Number of files

0

Curated

Created at: 04/16/2026 10:45:00:156

+ Create

Item

Files #

json-master-3fe18 (NOASSERTION)

0

75c946-3.0.0 (NOASSERTION)

0

75c946-0 (NOASSERTION)

0

checkout-6..75c946.*.* (NOAS..)

0

compiler-75c946-0 (NOASSER..)

0

create-github-app-token-3..75c9..

0

http-75c946-0 (NOASSERTION)

0

ip-75c946-0 (NOASSERTION)

0

rubyversions.yml-master-75c946..

0

setup-ruby-plugs-1..75c9461.*.*

0

trigger-workflow-and-wait-1.6.5..

0

unit-75c946-0 (NOASSERTION)

0

unit-ruby-core-75c946-0 (NOA..)

0



4.17.6.4 Httparty

<https://github.com/jnunemaker/httparty>

SBOM Mgmt

Choose project

jnunemaker_httparty - 383521

Search files...

Show all

Files

Overview

Copyrights (0)

Licenses (3)

License	Number in software components
MIT	1
Ruby	1
GPL 2.0-only	1

Vulnerabilities (0)

+ Create

Item

Files #

httparty-main-88171b (MIT)

1.2.0.pre2-75c946 (Ruby OR GPL 2.0 o..)

75c946--> 2.3 (NOASSERTION)

75c946--> 3.4 (NOASSERTION)

75c946--> 0 (NOASSERTION)

75c946--> 0.5.2 (NOASSERTION)

75c946--> 1.0.0 (NOASSERTION)

bundler-75c946--> 0 (NOASSERTION)

checkout-4..75c946.*.* (NOASSERTI..)

rspec-75c946--> 0 (NOASSERTION)

setup-ruby-1..75c9461.*.* (NOASSERTI..)

Vulnerabilities

Choose project

jnunemaker_httparty

Filter

2 rows

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
VCOB-66f6-3cnu-aaae	CVE-2007-4612, GHSA-m76-43v2-49vf	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCOB-66f6-3cnu-aaae	False	04/15/2026 15:47:07:013
VCOB-d61-76r6-aaaf	CVE-2013-0175, GHSA-pctc-949f-53m5, OSV-89148	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCOB-d61-76r6-aaaf	False	04/15/2026 15:47:09:239

+ Create Edit Remove

Excel JSON



Software components

Choose project

jrunemaker_httparty -

> Filter

11 rows

Name	Version	PURL	Licenses	Curated	License controlled by AI
pry	=> 0	pkg:gem/pry		False	
guard-rspec	=> 0	pkg:gem/guard-rspec		False	
guard-bundler	=> 0	pkg:gem/guard-bundler		False	
rspec	=> 3.4	pkg:gem/rspec		False	
cucumber	=> 2.3	pkg:gem/cucumber		False	
mongrel	1.2.0.pre2	pkg:gem/mongrel@1.2.0.pre2	Ruby, GPL-2.0-only	False	
multi_xml	=> 0.5.2	pkg:gem/multi_xml		False	
mini_mime	=> 1.0.0	pkg:gem/mini_mime		False	
actions/checkout	4.**	pkg:githubactions/actions/checkout@4.%2A.%2A		False	
ruby/setup-ruby	1.**	pkg:githubactions/ruby/setup-ruby@1.%2A.%2A		False	
com.github.jrunemaker/httparty	main	pkg:github/jrunemaker/httparty@main	MIT	False	

+ Create Edit Remove

Inventory

Choose project

jrunemaker_httparty -

> Filter

11 rows

Inventory name	Software component	Size	Linking	Curated
bundler-75c946--0 (NOASSERTION)	guard-bundler	0		False
75c946--3.4 (NOASSERTION)	rspec	0		False
75c946--2.3 (NOASSERTION)	cucumber	0		False
rspec-75c946--0 (NOASSERTION)	guard-rspec	0		False
1.2.0.pre2-75c946 (Ruby OR GPL-2.0-only)	mongrel	0		False
75c946--0.5.2 (NOASSERTION)	multi_xml	0		False
75c946--1.0.0 (NOASSERTION)	mini_mime	0		False
checkout-4..75c9464.** (NOASSERTION)	actions/checkout	0		False
setup-ruby-1..75c9461.** (NOASSERTION)	ruby/setup-ruby	0		False
httparty-main-88171b (MIT)	com.github.jrunemaker/httparty	0		False
75c946--0 (NOASSERTION)	pry	0		False

+ Create Edit Remove

<https://github.com/lostisland/faraday>

OCCTET Deliverable Number: D 3.3 - SME Toolkit-Demo-Del - page 145



OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

+

SBOM Mgmt

Choose project

Faraday - 378

Search files...

Show all

Files

Overview

Inventory items

75c946>= 0 (NOASSERTION)

Inventory item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Filter

Resolved	ID	Aliases	Severity	Exploitability	Risk score
☒	VCID-9tms-q5u9-hqg5	CVE-2026-33210, GHSA-3m6g-2423-7cp3	Medium	0.5	4
☒	VCID-dtbn-dg3w-aaap	CVE-2013-0269, GHSA-x457-cw4h-hq5f, OSV-101137	Medium	0.5	4
☒	VCID-t5p8-75v9-aaap	CVE-2020-10663, GHSA-jhgq-qwrw-7w9g	Medium	0.5	4

Update vulnerabilities

Create VEX | Confirm

+ Create

Vulnerable

Files #

1.2.9-b457d0 (MIT)

0

0

0

75c946>= 0 (NOASSERTION)

0

0

0

9.6.0-5b6e42 (MIT)

0

0

0

openssl-75c946--> 0.11.0 (NOASSERTION)

0

0

0

openssl-75c946--> 0.11.0 (NOASSERTION)

0

0

0

openssl-75c946--> 0.11.0 (NOASSERTION)

0

0

0

OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

+

Vulnerabilities

Choose project

Faraday - 378

Filter

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
VCID-9tms-hqth-aaaf	GHSA-845c-c33v-vp6g, GMS-2023-285	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCID-9tms-hqth-aaaf	False	04/16/2025 10:01:32.432
VCID-232e-v1m1-aaan	CVE-2022-33987, GHSA-pfrx-2q88-qd97	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VCID-232e-v1m1-aaan	False	04/16/2025 10:01:48.937
VCID-6r6d-b4d3-aaak	CVE-2022-21680, GHSA-nrm-qgm4-v8hf	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCID-6r6d-b4d3-aaak	False	04/16/2025 10:02:47.774
VCID-cvth-cwus-aaan	CVE-2021-21306, GHSA-462-v4qz-hr96	Low	0.5	3.4	http://public.vulnerablecode.io/vulnerabilities/VCID-cvth-cwus-aaan	False	04/16/2025 10:02:48.108
VCID-q5f4-ut36-aaac	CVE-2022-21681, GHSA-5v2h-zc3x-5uqj	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCID-q5f4-ut36-aaac	False	04/16/2025 10:03:39.982
VCID-ekjb-tg1g-aaas	CVE-2021-3807, GHSA-93g8-gd89-wgmw	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCID-ekjb-tg1g-aaas	False	04/16/2025 10:03:14.510
VCID-9tms-q5u9-hqg5	CVE-2026-33210, GHSA-3m6g-2423-7cp3	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCID-9tms-q5u9-hqg5	False	04/16/2025 10:03:39.982
VCID-dtbn-dg3w-aaap	CVE-2013-0269, GHSA-x457-cw4h-hq5f, OSV-101137	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCID-dtbn-dg3w-aaap	False	04/16/2025 10:03:39.982
VCID-t5p8-75v9-aaap	CVE-2020-10663, GHSA-jhgq-qwrw-7w9g	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCID-t5p8-75v9-aaap	False	04/16/2025 10:03:39.982
VCID-hc96-7azw-8qth	CVE-2025-46551, GHSA-72qg-48q4-5qpx	Low	0.5	3.1	http://public.vulnerablecode.io/vulnerabilities/VCID-hc96-7azw-8qth	False	04/16/2025 10:03:58.201
VCID-v7m-bbpt-aaan	CVE-2009-4123, GHSA-xyz7-pqg8-h2w9	Medium	0.5	4	http://public.vulnerablecode.io/vulnerabilities/VCID-v7m-bbpt-aaan	False	04/16/2025 10:03:58.488

+ Create

Edit

Remove

Excel

JSON

OCCTET Deliverable Number: D 3.3 - SME Toolkit-Demo-Del - page 147



4.17.6.6 Guard

<https://github.com/guard/guard>

localhost:8090/boc/audit-view/102

SBOM Mgmt

Choose project
guard_guard_d4042e - d4042e

Search files... 0/0

Show all

Files 0

Overview

> Copyrights (0)

> Licenses (1)

License	Number in software components
MIT	2

> Vulnerabilities (1)

+ Create

Item Files #

guard-master-ef5757 (MIT)	0
0.83.0-75c946 (MIT)	0
75c946--> 0.0 (NOASSERTION)	0
75c946--> 0.1 (NOASSERTION)	0
75c946--> 0.14 (NOASSERTION)	0
75c946--> 1.6 (NOASSERTION)	0
75c946--> 0 (NOASSERTION)	0
75c946--> 0.0.0 (NOASSERTION)	0
75c946--> 0.13.0 (NOASSERTION)	0
75c946--> 0.18.1 (NOASSERTION)	0
75c946--> 0.2.4 (NOASSERTION)	0
75c946--> 1.0.12 - 2.0 (NOASSERTION)	0
75c946--> 2.7 - 4.0 (NOASSERTION)	0
75c946--> 3.0.0 (NOASSERTION)	0
checkout-master-75c946 (NOASSERTION)	0
coverage-75c946--> 0 (NOASSERTION)	0
cucumber-75c946--> 2.1 (NOASSERTION)	0
release-drafter-5.2.0-75c946 (NOASSER...	0
rome-75c946--> 0 (NOASSERTION)	0
rspec-75c946--> 0 (NOASSERTION)	0
rubocop-75c946--> 0 (NOASSERTION)	0

localhost:8090/boc/vulnerabilities

Vulnerabilities

Choose project
guard_guard_d4042e - i

> Filter

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
VGD-Skr-Sppb-n7d	CVE-2025-54314, GHSA-mgcp-p2hv-vwfx	Medium	0.5	4	http://public.vulnerabilitycode.io/vulnerabilities/VGD-Skr-Sppb-n7d	False	04/15/2026 15:40:54.000

+ Create Edit Remove

Excel JSON



Software components

Choose project

guard_guard_d4042e - 1

> Filter

<< 21 rows >>

Name	Version	PURL	Licenses	Curated	License controlled by AI
logger	→ 1.6	pkg:gem/logger		False	
actions/checkout	master	pkg:githubactions/actions/checkout@master		False	
toolmantim/release-drafter	5.2.0	pkg:githubactions/toolmantim/release-drafter@5.2.0		False	
com.github.guard/guard	master	pkg:github/guard/guard@master	MIT	False	
netic	→ 0	pkg:gem/netic		False	
rspec	→ 3.0.0	pkg:gem/rspec		False	
guard-ronn	→ 0	pkg:gem/guard-ronn		False	
guard-rubocop	→ 0	pkg:gem/guard-rubocop		False	
aruba	→ 0.14	pkg:gem/aruba		False	
rubocop	0.83.0	pkg:gem/rubocop@0.83.0	MIT	False	
rubinius-coverage	→ 0	pkg:gem/rubinius-coverage		False	
guard-rspec	→ 0	pkg:gem/guard-rspec		False	
guard-cucumber	→ 2.1	pkg:gem/guard-cucumber		False	
notiffany	→ 0.0.6	pkg:gem/notiffany		False	
listen	→ 2.7.4.0	pkg:gem/listen		False	
formatador	→ 0.2.4	pkg:gem/formatador		False	
newr	→ 0.1	pkg:gem/newr		False	
pry	→ 0.13.0	pkg:gem/pry		False	
lumberjack	→ 1.0.12, 2.0	pkg:gem/lumberjack		False	
thor	→ 0.18.1	pkg:gem/thor		False	
shellany	→ 0.0	pkg:gem/shellany		False	

+ Create Edit Remove

Inventory

Choose project

guard_guard_d4042e - 1

> Filter

<< 21 rows >>

Inventory name	Software component	Size	Linking	Curated
guard-master-e6b707 (MIT)	com.github.guard/guard	0		False
rubocop-75c946→ 0 (NOASSERTION)	guard-rubocop	0		False
cucumber-75c946→ 2.1 (NOASSERTION)	guard-cucumber	0		False
coverage-75c946→ 0 (NOASSERTION)	rubinius-coverage	0		False
75c946→ 3.0.0 (NOASSERTION)	rspec	0		False
ronn-75c946→ 0 (NOASSERTION)	guard-ronn	0		False
75c946→ 0.14 (NOASSERTION)	aruba	0		False
0.83.0-75c946 (MIT)	rubocop	0		False
rspec-75c946→ 0 (NOASSERTION)	guard-rspec	0		False
75c946→ 0.0.6 (NOASSERTION)	notiffany	0		False
75c946→ 2.7.4.0 (NOASSERTION)	listen	0		False
75c946→ 0.2.4 (NOASSERTION)	formatador	0		False
75c946→ 0.1 (NOASSERTION)	newr	0		False
75c946→ 0.13.0 (NOASSERTION)	pry	0		False
75c946→ 1.0.12, 2.0 (NOASSERTION)	lumberjack	0		False
75c946→ 0.18.1 (NOASSERTION)	thor	0		False
75c946→ 0.0 (NOASSERTION)	shellany	0		False
75c946→ 1.6 (NOASSERTION)	logger	0		False
checkout-master-75c946 (NOASSERTION)	actions/checkout	0		False
release-drafter-5.2.0-75c946 (NOASSERTION)	toolmantim/release-drafter	0		False
75c946→ 0 (NOASSERTION)	netic	0		False

+ Create Edit Remove



4.17.6.7 Thor

<https://github.com/rails/thor>

Occtet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities
- VEX listing
- Projects
- Software components**
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration
 - Configuration
 - Organizations
 - Services
 - Users
 - Backend logs

Software components

Choose project
Rails_Thor - a8f534

> Filter

Name	Version	PURL	Licenses	Curated	License controlled by AI
ruby/setup-ruby	1.**	pkg.githubactions/ruby/setup-ruby@1.%2A.%2A		False	
actions/checkout	6.**	pkg.githubactions/actions/checkout@6.%2A.%2A		False	
pry	>= 0	pkg.gem/pry		False	
rubgems/configure-rubgems-credentials	1.0.0	pkg.githubactions/rubgems/configure-rubgems-cred...		False	
webmock	>= 3.14	pkg.gem/webmock		False	
pry-byebug	>= 0	pkg.gem/pry-byebug		False	
rubocop	>= 1.30	pkg.gem/rubocop		False	
coveralls-rsborn	>= 0.23.1	pkg.gem/coveralls-rsborn		False	
rspec	>= 3.2	pkg.gem/rspec		False	
rspec-mocks	>= 3	pkg.gem/rspec-mocks		False	
simplecov	>= 0.13	pkg.gem/simplecov		False	
bundler	>= 1.0	pkg.gem/bundler		False	
com.github.rails:thor	main	pkg.githubrails/thor@main	MIT	False	

+ Create Edit Remove

Occtet Curator

- Dashboard
- SBOM Mgmt**
- Vulnerabilities
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration
 - Configuration
 - Organizations
 - Services
 - Users
 - Backend logs

SBOM Mgmt

Choose project
Rails_Thor - a8f534

Search files...

Show all

Files

Overview

> Copyrights (0)

> Licenses (1)

License	Number in software components
MIT	1

> Vulnerabilities (0)

+ Create

Item Files #

- thor-main-9a9c5a (MIT) 0
- 75c946--> 0.23.1 (NOASSERTION) 0
- 75c946--> 1.30 (NOASSERTION) 0
- 75c946--> 0 (NOASSERTION) 0
- 75c946--> 0.13 (NOASSERTION) 0
- 75c946--> 1.0 (NOASSERTION) 0
- 75c946--> 3.2 (NOASSERTION) 0
- 75c946--> 3.14 (NOASSERTION) 0
- 75c946--> 0 (NOASSERTION) 0
- byebug-75c946--> 0 (NOASSERTION) 0
- checkout-6-75c946.** (NOAS... 0
- configure-rubgems-credentials-... 0
- mocks-75c946--> 3 (NOASSERTION) 0
- setup-ruby-1-75c946.** (NOA... 0



OCCTET Curator

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT Issues
ORT Violation
Import
Help
Administration

[admin]

SBOM Mgmt

Choose project

Rails_Thor - a8f534

Search files...

Show all

Files

Overview

Inventory items

75c946-> 1.30 (NOASSERTION)

Inventory item

Inventory name

75c946-> 1.30 (NOASSERTION)

Parent inventory item

thor-main-9a9c5a (MIT)

Software component

rubocop

Download URL

NOASSERTION

Linking

Priority

Number of files

0

Curated

Created at: 04/16/2026 10:30:29:640

+ Create

Item

Files #

thor-main-9a9c5a (MIT)	0
75c946-> 0.23.1 (NOASSERTION)	0
75c946-> 1.30 (NOASSERTION)	0
75c946-> 0 (NOASSERTION)	0
75c946-> 0.13 (NOASSERTION)	0
75c946-> 1.0 (NOASSERTION)	0
75c946-> 3.14 (NOASSERTION)	0
75c946-> 3.2 (NOASSERTION)	0
byetug-75c946-> 0 (NOASERTI...	0
checkout-6-75c946-.* (NOAS...	0
configure-rubygems-credentials...	0
mocks-75c946-> 3 (NOASERTI...	0
setup-ruby-1-75c946-.* (NOA...	0

OCCTET Curator

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT Issues
ORT Violation
Import
Help
Administration

[admin]

Vulnerabilities

Choose project

Rails_Thor - a8f534

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

+ Create

Edit

Remove

Excel

JSON



Octet Curator

SBOM Mgmt

Choose project: **Rails_Thor - a8f534**

Search files... **0**

Show all

Files

Overview Inventory items

> Copyrights (0)

> Licenses (1)

> Vulnerabilities (0)

Vulnerability Risk score of vulnerability Number in software components

Item Files #

thor-main-9a6c5a (MIT) 0

75c946--> 0.23.1 (NOASSERTION) 0

75c946--> 1.30 (NOASSERTION) 0

75c946--> 0 (NOASSERTION) 0

75c946--> 0.13 (NOASSERTION) 0

75c946--> 1.0 (NOASSERTION) 0

75c946--> 3.14 (NOASSERTION) 0

75c946--> 3.2 (NOASSERTION) 0

bootstrap-75c946--> 0 (NOASSERTION) 0

checkout-6-75c946- ** (NOAS... 0

configure-rubygems-credentials-... 0

mocks-75c946--> 3 (NOASERTI... 0

setup-ruby-1-75c9461- ** (NOA... 0

[admin]

4.17.6.8 Rest-client

<https://github.com/rest-client/rest-client>

Octet Curator

Software components

Choose project: **Rest-Client - 378d4e**

Filter

13 rows

Name	Version	PURL	Licenses	Curated	License controlled by AI
rake	>= 0	pkg:gem/rake		False	
netrc	>= 0.8	pkg:gem/netrc		False	
pry	>= 0	pkg:gem/pry		False	
http-accept	>= 1.7.0, < 2.0	pkg:gem/http-accept		False	
http-cookie	>= 1.0.2, < 2.0	pkg:gem/http-cookie		False	
mime-types	>= 1.16, < 4.0	pkg:gem/mime-types		False	
rspec	>= 3.0	pkg:gem/rspec		False	
rubocop	>= 0.49	pkg:gem/rubocop		False	
webmock	>= 2.0	pkg:gem/webmock		False	
pry-doc	>= 0	pkg:gem/pry-doc		False	
rdoc	>= 2.4.2, < 6.0	pkg:gem/rdoc		False	
ffi	>= 1.9	pkg:gem/ffi		False	
com.github.rest-client/rest-client	master	pkg:github/rest-client/rest-client#master	MIT	False	

[admin]

+ Create Edit Remove



OCCTET Curator

SBOM Mgmt

Choose project

Rest-Client - 378d4e

Search files...

Show all

Files

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

Overview

Inventory items

> Copyrights (0)

> Licenses (1)

License

MIT

Number in software components

1

> Vulnerabilities (0)

+ Create

Item

Expand all

Files #

client-rest-client-master-92c252 (MIT)

0

▲

75c946--> 0 (NOASSERTION)

0

▲

75c946--> 0.49 (NOASSERTION)

0

▲

75c946--> 0.8 (NOASSERTION)

0

▲

75c946--> 1.9 (NOASSERTION)

0

▲

75c946--> 2.0 (NOASSERTION)

0

▲

75c946--> 3.0 (NOASSERTION)

0

▲

75c946--> 2.4.2+ 6.0 (NOASSER...

0

▲

accept-75c946-- 1.7.0+ 2.0 (NO...

0

▲

cookie-75c946-- 1.0.2+ 2.0 (NO...

0

▲

doc-75c946--> 0 (NOASSERTION)

0

▲

types-75c946-- 1.16+ 4.0 (NOA...

0

▲

OCCTET Curator

SBOM Mgmt

Rest-Client - 378d4e

Search files...

Show all

Files

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

Overview

Inventory items

75c946--> 1.9 (NOASSERTION) ✕

Inventory item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Inventory name

75c946--> 1.9 (NOASSERTION)

Parent inventory item

client-rest-client-master-92c252 (MIT)

Software component

fit

Download URL

NOASSERTION

Linking

Priority

Number of files

0

Curated

Created at: 04/16/2026 10:39:18:235

+ Create

Item

Expand all

Files #

client-rest-client-master-92c252 (MIT)

0

▲

75c946--> 0 (NOASSERTION)

0

▲

75c946--> 0.49 (NOASSERTION)

0

▲

75c946--> 0.8 (NOASSERTION)

0

▲

75c946--> 1.9 (NOASSERTION)

0

▲

75c946--> 2.0 (NOASSERTION)

0

▲

75c946--> 3.0 (NOASSERTION)

0

▲

75c946--> 2.4.2+ 6.0 (NOASSER...

0

▲

accept-75c946-- 1.7.0+ 2.0 (NO...

0

▲

cookie-75c946-- 1.0.2+ 2.0 (NO...

0

▲

doc-75c946--> 0 (NOASSERTION)

0

▲

types-75c946-- 1.16+ 4.0 (NOA...

0

▲



OCCTET Curator

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT Issues
ORT Violation
Import
Help
Administration
Configuration
Organizations
Services
Users
Backend logs

[admin]

SBOM Mgmt

Choose project

Rest-Client - 378d4e

Search files...

Show all

Files

Overview

Inventory items

Copyrights (0)

Licenses (1)

Vulnerabilities (0)

Vulnerability

Risk score of vulnerability

Number in software components

+ Create

Item

Files #

client-rest-client-master-92c232 (MIT)

0

▲

75c946--> 0 (NOASSERTION)

0

▲

75c946--> 0.49 (NOASSERTION)

0

▲

75c946--> 0.8 (NOASSERTION)

0

▲

75c946--> 1.9 (NOASSERTION)

0

▲

75c946--> 2.0 (NOASSERTION)

0

▲

75c946--> 3.0 (NOASSERTION)

0

▲

75c946--> 0 (NOASSERTION)

0

▲

75c946--> 2.42+ 6.0 (NOASER...

0

▲

accept-75c946--> 1.7.8+ 2.0 (NO...

0

▲

cookie-75c946--> 1.0.2+ 2.0 (NO...

0

▲

doc-75c946--> 0 (NOASSERTION)

0

▲

types-75c946--> 1.16+ 4.0 (NOA...

0

▲

OCCTET Curator

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT Issues
ORT Violation
Import
Help
Administration
Configuration
Organizations
Services
Users
Backend logs

[admin]

Vulnerabilities

Choose project

Rest-Client - 378d4e

Filter

ID

Aliases

Severity

Exploitability

Risk score

Source URL

Manually created

Last update

VDID-ftgh-jkwa-saab

CVE-2020-11023, GHSA-jpcz-cgw5-v4f6

Critical

2

10

http://public.vulnerablecode.io/vulnerabilities/VDID-ftgh-jkwa-saab

False

04/16/2025 10:13:21:233

VDID-42m-mjbg-saab

CVE-2020-8130, GHSA-pgn-qw3-w3q8

Low

0.5

3.1

http://public.vulnerablecode.io/vulnerabilities/VDID-42m-mjbg-saab

False

04/16/2025 10:34:24:802

VDID-8ub-q56-saab

CVE-2017-8418, GHSA-wmf-jg3-9f3

Low

0.5

1.5

http://public.vulnerablecode.io/vulnerabilities/VDID-8ub-q56-saab

False

04/16/2025 10:46:17:769

VDID-j62-g1k3-saab

CVE-2018-1000201, GHSA-2gw2-8qfw-cwfp

Medium

0.5

4

http://public.vulnerablecode.io/vulnerabilities/VDID-j62-g1k3-saab

False

04/16/2025 10:47:49:209

+ Create

Edit

Remove

Excel

JSON



SBOM Mgmt

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

Choose project

Rest-Client - 378d4e

Search files...

Show all

Files

Overview

Inventory items

Copyrights (0)

Licenses (1)

Vulnerabilities (4)

Vulnerability	Risk score of vulnerability	Number in software components
VCD-Rhgh-jkwa-aaah	10	1
VCD-d2m-mjbp-aaaj	3.1	1
VCD-Rubq-rt5d-aaab	1.5	1
VCD-R62-q1k3-aaaj	4	1

Create

Item	Files #
client-rest-client-master-92c252 (MIT)	0
75c946--> 0 (NOASSERTION)	0
75c946--> 0.49 (NOASSERTION)	0
75c946--> 0.8 (NOASSERTION)	0
75c946--> 1.9 (NOASSERTION)	0
75c946--> 2.0 (NOASSERTION)	0
75c946--> 3.0 (NOASSERTION)	0
75c946--> 0 (NOASSERTION)	0
75c946--> 2.4.2, 6.0 (NOASER..	0
accept-75c946--> 1.7.0, 2.0 (NO..	0
cookie-75c946--> 1.0.2, 2.0 (NO..	0
doc-75c946--> 0 (NOASSERTION)	0
types-75c946--> 1.16, 4.0 (NOA..	0

Choose project

Rest-Client - 378d4e

Search files...

Show all

Files

Overview

Inventory items

75c946--> 1.9 (NOASSERTION)

75c946--> 0.49 (NOASSERTION)

Inventory item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Filter

Resolved	ID	Aliases	Severity	Exploitability	Risk score
☐	VCD-Rubq-rt5d-aaab	CVE-2017-8418, GHSA-wmfp-ggij-9f3	Low	6.5	1.5

Update vulnerabilities

Create VEX

Create

Item	Files #
client-rest-client-master-92c252 (MIT)	0
75c946--> 0 (NOASSERTION)	0
75c946--> 0.49 (NOASSERTION)	0
75c946--> 0.8 (NOASSERTION)	0
75c946--> 1.9 (NOASSERTION)	0
75c946--> 2.0 (NOASSERTION)	0
75c946--> 3.0 (NOASSERTION)	0
75c946--> 0 (NOASSERTION)	0
75c946--> 2.4.2, 6.0 (NOASER..	0
accept-75c946--> 1.7.0, 2.0 (NO..	0
cookie-75c946--> 1.0.2, 2.0 (NO..	0
doc-75c946--> 0 (NOASSERTION)	0
types-75c946--> 1.16, 4.0 (NOA..	0



4.17.6.9 Rack

<https://github.com/rack/rack>

Octet Curator

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT Issues
ORT Violation
Import
Help
Administration
Configuration
Organizations
Services
Users
Backend logs

[admin]

SBOM Mgmt

Choose project

Rack - 0F7952

Search files...

Show all

Files

rack

main

bin

rackup

control

rack_logo.svg

example

lobster.ru

protectedlobster.rb

protectedlobster.ru

lib

rack

rack.rb

test

cgi

multipart

rackup

unregistered_handler

gemloader.rb

spec_rack_auth_basic.rb

spec_rack_auth_digest.rb

spec_rack_builder.rb

spec_rack_camping.rb

spec_rack_cascade.rb

spec_rack_cgi.rb

Overview

Inventory items

Copyrights (0)

Licenses (0)

Vulnerabilities (1)

Vulnerability	Risk score of vulnerability	Number in software components
VCD:high:jwaa-aaah	10	1

+ Create

Item

Files #

rack-main-98ebb6 (NOASSERTION)	0
75c946-5 (NOASSERTION)	0
75c946-0 (NOASSERTION)	0
checkout-6..75c9466.** (NOAS...	0
dependency-review action-4..75...	0
deploy pages-5..75c9465.** (N...	0
globalexpectations-75c946-0 (...)	0
packaging-75c946-0 (NOASSE...	0
setup-ruby-1..75c9461.** (NOA...	0
setup-ruby-pkgs-1..75c9461.** ..	0
test-external-75c946-0 (NOAS...	0
upload-pages-artifact-4..75c946...	0

SBOM Mgmt

Choose project

Rack - 0F7952

Search files...

Show all

Files

rack

main

bin

rackup

control

rack_logo.svg

example

lobster.ru

protectedlobster.rb

protectedlobster.ru

lib

rack

rack.rb

test

cgi

multipart

rackup

unregistered_handler

gemloader.rb

spec_rack_auth_basic.rb

spec_rack_auth_digest.rb

spec_rack_builder.rb

spec_rack_camping.rb

spec_rack_cascade.rb

spec_rack_cgi.rb

Overview

Inventory items

75c946-0 (NOASSERTION)

Inventory item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Inventory name

75c946-0 (NOASSERTION)

Parent inventory item

rack-main-98ebb6 (NOASSERTION)

Software component

rdoc

Download URL

NOASSERTION

Linking

Priority

Number of files

0

Curated

Created at: 04/16/2026 10:12:52:527

+ Create

Item

Files #

rack-main-98ebb6 (NOASSERTION)	0
75c946-5 (NOASSERTION)	0
75c946-0 (NOASSERTION)	0
checkout-6..75c9466.** (NOAS...	0
dependency-review action-4..75...	0
deploy pages-5..75c9465.** (N...	0
globalexpectations-75c946-0 (...)	0
packaging-75c946-0 (NOASSE...	0
setup-ruby-1..75c9461.** (NOA...	0
setup-ruby-pkgs-1..75c9461.** ..	0
test-external-75c946-0 (NOAS...	0
upload-pages-artifact-4..75c946...	0



Octet Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

SBOM Mgmt

Choose project

Rack - 0F7952

Search files...

Show all

Files

rack

main

bin

rackup

contrib

rack_logs.svg

example

lobster.ru

protectedlobster.rb

protectedlobster.ru

lib

rack

rack.rb

test

cgi

multipart

rackup

unregistered_handler

gemloader.rb

spec_rack_auth_basic.rb

spec_rack_auth_digest.rb

spec_rack_builder.rb

spec_rack_camping.rb

spec_rack_cascade.rb

spec_rack_cgi.rb

Overview

Inventory items

75c946>= 0 (NOASSERTION)

Inventory item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Filter

Resolved

ID

Aliases

Severity

Exploitability

Risk score

VCD-thgh-jkwa-aaah

CVE-2020-11023, GHSA-jpcq-cgw6-v4f6

Critical

2

10

Update vulnerabilities

Create VEX

+ Create

Item

Files

rack-main/8eb6b (NOASSERTION)

75c946= 5 (NOASSERTION)

75c946= 8 (NOASSERTION)

checkout 4..75c946.*.* (NOAS...

dependency-review-action-4..75...

deploy pages 5..75c9465.*.* (N...

globalexpectations-75c946= 0 (...)

packaging-75c946= 0 (NOASSE...

setup-ruby-1..75c9461.*.* (NOA...

setup-ruby-plugs-1..75c9461.*.*...

test-external-75c946= 0 (NOAS...

upload pages artifact 4..75c946...

Octet Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

Vulnerabilities

Choose project

Rack - 0F7952

VEX listing

Filter

ID

Aliases

Severity

Exploitability

Risk score

Source URL

Manually created

Last update

VCD-thgh-jkwa-aaah

CVE-2020-11023, GHSA-jpcq-cgw6-v4f6

Critical

2

10

http://public.vulntracode.io/vulnerabilities/VCD-thgh-jkwa-aaah

False

04/16/2026 10:13:31.233

+ Create

Edit

Remove

Excel

JSON



Octet Curator

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT Issues
ORT Violation
Import
Help
Administration
Configuration
Organizations
Services
Users
Backend logs

Software components

Choose project
Rack - 0F7952

> Filter

12 rows

Name	Version	PURL	Licenses	Curated	License controlled by AI
ruby/setup-ruby	1.**	pkg.githubactions/ruby/setup-ruby@1.52A.52A		False	
actions/checkout	6.**	pkg.githubactions/actions/checkout@6.52A.52A		False	
rubocop-packaging	>= 0	pkg.gem/rubocop-packaging		False	
bake-test-external	>= 0	pkg.gem/bake-test-external		False	
rdoc	>= 0	pkg.gem/rdoc		False	
minitest	> 5	pkg.gem/minitest		False	
minitest-global_expectations	>= 0	pkg.gem/minitest-global_expectations		False	
actions/dependency-review-action	4.**	pkg.githubactions/actions/dependency-review-action@4.52A.52A		False	
actions/upload-pages-artifact	4.**	pkg.githubactions/actions/upload-pages-artifact@4.52A.52A		False	
actions/deploy-pages	5.**	pkg.githubactions/actions/deploy-pages@5.52A.52A		False	
ruby/setup-ruby-pkgs	1.**	pkg.githubactions/ruby/setup-ruby-pkgs@1.52A.52A		False	
com.github.rack/rack	main	pkg.github/rack/rack@main		False	

+ Create
Edit
Remove

[admin]

4.17.6.10 Sqlite3-ruby

<https://github.com/sparklemotion/sqlite3-ruby>

Octet Curator

Dashboard
SBOM Mgmt
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT Issues
ORT Violation
Import
Help
Administration
Configuration
Organizations
Services
Users
Backend logs

SBOM Mgmt

Choose project
Sparklemotion_Sqlite3 - 651b4

Search files...
Show all
Files

Overview

> Copyrights (0)

> Licenses (7)

License	Number in software components
MIT	7
BSD-3-Clause	2
Ruby	1
GPL-1.0-or-later	1
ORL-1.1	1
Unknown	1
Artistic-1.0-Pperl	1

> Vulnerabilities (0)

+ Create

Item

Files #

sqlite3-ruby-main-0784b (BSD-3-Clause) 0
1.33.0-75c946 (MIT) 0
1.59.0-75c946 (MIT) 0
6.0.3-75c946 (MIT) 0
7.2.0-75c946 ((BSD-3-Clause AND NOASSERTION)) 0
75c946--> 2.8.0 (NOASSERTION) 0
cache-68822822ae0a0e4a088... 0
checkout-de0fac2e4500da0e000... 0
compiler-1.3.1-75c946 (MIT) 0
compiler-dock-1.11.1-75c946 (M... 0
configure-pages-43f60f192ca1f... 0
configure-rubygems-credentials... 0
deploy-pages-cd2e8fcb37097... 0
download-artifact-3e54592c7b9... 0
freebsd-vim-7ca02799c3078fcd... 0
minitest-0.34.5-75c946 (MIT) 0
setup-ruby-455c17816e57e4815... 0
setup-ruby-pkgs-2233d37c1315c... 0
upload-artifact-0430846d1af3c7... 0
upload-pages-artifact-1c2240f54... 0

[admin]



OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

SBOM Mgmt

Choose project

Sparklemotion_Sqlite3 - 651b4

Search files...

Show all

Files

Overview

Inventory items

1.33.0-75c946 (MIT)

Inventory item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Inventory name

1.33.0-75c946 (MIT)

Parent inventory item

sqlite3-ruby-main-0784fb (BSD-3-Clause)

Software component

standard

Download URL

NOASSERTION

Linking

Priority

Number of files

0

Curated

Created at: 04/16/2026 11:04:27:482

+ Create

Item

Files

sqlite3-ruby-main-0784fb (BSD-3-Clause)

1.33.0-75c946 (MIT)

1.39.0-75c946 (MIT)

6.0.3-75c946 (MIT)

7.2.0-75c946 (MIT)

75c946--> 2.8.0 (NOASSERTION)

cache-668228422ae6a0fe4ad8f...

checkout-defracc3e4590dab00...

compiler-1.3.1-75c946 (MIT)

compiler-dock-1.11.1-75c946 (M...

configure-pages-436d0192ca1f...

configure-rubygems-credentials...

deploy-pages-c52c8f8c39697...

download-artifact-3e5f492c0b...

freebsd-vim-7ca2079e070fedc...

minitest-0.34.5-75c946 (MIT)

setup-ruby-e65c17d16e37e6815...

setup-ruby-pkg-2233d39c7315c...

upload-artifact-043b9461a93c7...

upload-pages-artifact-R-324d354...

OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Configuration

Organizations

Services

Users

Backend logs

[admin]

Vulnerabilities

Choose project

motion_Sqlite3 - 651b4

ID

Aliases

Severity

Exploitability

Risk score

Source URL

Manually created

Last update

+ Create

Edit

Remove

Export

JSON



Software components

Choose project: **motion_Sqllite3 - 651b4**

Filter

Name	Version	PURL	Licenses	Curated	License controlled by AI
rake-compiler-dock	1.11.1	pkg:gem/rake-compiler-dock@1.11.1	MIT	False	False
rake-compiler	1.3.1	pkg:gem/rake-compiler@1.3.1	MIT	False	False
ruby/setup-ruby	e65c17d16e57481588a5a0282698790082982	pkg:githubactions/ruby/setup-ruby@e65c17d16e57481...		False	False
actions/upload-artifact	043b461af3c77aa556e7c1c4a8f75d1f6a9a	pkg:githubactions/actions/upload-artifact@043b461...		False	False
actions/checkout	de0fac2a4500a0a0099e7214895447c636d	pkg:githubactions/actions/checkout@de0fac2a4500a...		False	False
actions/cache	668228422a4e4087e4d889e87c07199ec566a7	pkg:githubactions/actions/cache@668228422a4e408...		False	False
actions/download-artifact	3e54532c7b11725167a2970436418b326a5461a7c	pkg:githubactions/actions/download-artifact@3e545...		False	False
ruby/setup-ruby-pkgs	2233639c1315c67a2970436418b326a5461a7c	pkg:githubactions/ruby/setup-ruby-pkgs@2233639c13...		False	False
vmactions/freebsd-vm	7ca82f79638786cde653a2b094995447b0d	pkg:githubactions/vmactions/freebsd-vm@7ca82f796...		False	False
actions/configure-pages	45be0110ca1fae007ad9b0ae92b1680254a0d	pkg:githubactions/actions/configure-pages@45be011...		False	False
actions/deploy-pages	c02e8f3c39d7b0fca59f6a763bae58fa128	pkg:githubactions/actions/deploy-pages@c02e8f3c3...		False	False
actions/upload-pages-artifact	1c3240c5471047b6827a684c52872a11cc49c9	pkg:githubactions/actions/upload-pages-artifact@1c...		False	False
rubygems/configure-rubygems-credentials	bc6d2178ba4919d6825c6e470e821f5c44	pkg:githubactions/rubygems/configure-rubygems-cred...		False	False
rdoc	7.2.0	pkg:gem/rdoc@7.2.0	Artistic 1.9-Perl, GPL-1.1, Unknown, BSD-3-Clause, MIT, ...	False	False
minitest	6.0.3	pkg:gem/minitest@6.0.3	MIT	False	False
rubocop	1.59.0	pkg:gem/rubocop@1.59.0	MIT	False	False
standard	1.32.0	pkg:gem/standard@1.32.0	MIT	False	False
rubocop-minitest	0.34.5	pkg:gem/rubocop-minitest@0.34.5	MIT	False	False
mini_portile2	~> 2.8.0	pkg:gem/mini_portile2		False	False
com.github.sparklemotion/sqllite3-ruby	main	pkg:github/sparklemotion/sqllite3-ruby/main	BSD-3-Clause	False	False

[admin] + Create Edit Remove

4.17.7 JVM projects

4.17.7.1 Annotations 13.0

<https://mvnrepository.com/artifact/org.jetbrains/annotations/13.0>

SBOM Mgmt

Choose project: **org.jetbrains:annotations - 13**

Search files... Show all

Files

Overview **Inventory items**

Inventory item Vulnerabilities Files Audit notes Licenses Copyrights

Save

Inventory name: **\annotations-13.0-sources.jar**

Parent inventory item: **\annotations-13.0-sources.jar**

Software component: **\annotations-13.0-sources.jar**

Download URL: [Download](#)

Linking: **1** Curated

Created at: 04/20/2026 07:56:42:568

[curator-admin]



4.17.7.2 Com.google.code.findbugsjsr305-3.0.2

<https://mvnrepository.com/artifact/com.google.code.findbugs/jsr305/3.0.2>



Octet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities**
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration

Vulnerabilities

Choose project: **com.google.code.findb**

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

[curator-admin] [Create] [Edit] [Remove] [Excel] [JSON]

4.17.7.3 Listenablefuture-9999.0.empty-to-avoid-conflict-with-guava

<https://mvnrepository.com/artifact/com.google.guava/listenablefuture/9999.0-empty-to-avoid-conflict-with-guava>

Octet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration

SBOM Mgmt

Choose project: **com.google.guava.listenablefuture**

Search files... [0.0] [Show all]

Files

Overview **Inventory items**

Inventory item **Vulnerabilities** **Files** **Audit notes** **Licenses** **Copyrights** **Save**

Inventory name
\\listenablefuture-9999.0-empty-to-avoid-conflict-with-guava.jar

Parent inventory item **Software component**
\\listenablefuture-9999.0-empty-to-avoid-conflict-with-guava.jar

Download URL

Linking **Priority** **Number of files** **Curated**
1

Created at: 04/20/2026 08:02:04:321

Item **Files #**

- C:\Users\joshah\Downloads\Anchor... 0
- archive-listenablefuture-9999.0-empty-to-avoid-co... 0
- \\listenablefuture-9999.0-empty-to-avoid-co... 1



Octet Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Vulnerabilities

Choose project
com.google.guava:liste

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

+ Create

Edit

Remove

Excel

JSON

4.17.7.4 Commons-logging-1.2

<https://mvnrepository.com/artifact/commons-logging/commons-logging/1.2>

Octet Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

SBOM Mgmt

Choose project
commons-logging:commons-logging

Search files...
Show all

Files

Overview

Inventory Items

commons-logging-1.2-test-sources.jar

Inventory Item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Inventory name
commons-logging-1.2-test-sources.jar

Parent inventory item
commons-logging-1.2-test-sources.jar

Software component
commons-logging-1.2-test-sources.jar

Download URL

Linking
Priority
Number of files
1
Curated

Created at: 04/20/2026 07:59:03:057

+ Create

Item

Files

commons-logging-1.2-test-sources.jar

0-users-joshah-abah-Documents-Anchore-c-



OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Vulnerabilities

Choose project
commons-logging.com

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

curator-admin

Create

Edit

Remove

Excel

JSON

4.17.7.5 Guava-failureaccess-1.0.1

<https://mvnrepository.com/artifact/com.google.guava/failureaccess/1.0.1>

OCCTET Curator

Dashboard

SBOM Mgmt

Vulnerabilities

VEX listing

Projects

Software components

Inventory

Licenses

Copyrights

ORT Issues

ORT Violation

Import

Help

Administration

Vulnerabilities

Choose project
com.google.guava:failu

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

curator-admin

Create

Edit

Remove

Excel

JSON



Occtet Curator SBOM Mgmt

Choose project: **com.google.guava:failureaccess-1.0.1**

Search files... **Show all**

Files

Inventory items

Inventory name
failureaccess-1.0.1-sources.jar

Parent inventory item
[Dropdown]

Software component
failureaccess-1.0.1-sources.jar

Download URL
[Text field]

Linking [Dropdown] **Priority** [Text field] **Number of files** [Text field] ☐ Curated

Created at: 04/20/2026 07:59:28:650

4.17.7.6 Javax-inject-1

<https://mvnrepository.com/artifact/javax.inject/javax.inject/1>



The screenshot shows the 'Occtet Curator' application interface. On the left is a sidebar with navigation options: Dashboard, SBOM Mgmt, Vulnerabilities, VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT issues, ORT Violation, Import, Help, and Administration. The main area is titled 'SBOM Mgmt' and shows the 'Inventory items' form for the project 'javax.inject-1-sources.jar'. The form includes fields for 'Inventory name' (set to '\javax.inject-1-sources.jar'), 'Parent inventory item', 'Software component' (set to '\javax.inject-1-sources.jar'), and 'Download URL'. It also has a 'Linking' dropdown, 'Priority', 'Number of files' (set to 1), and a 'Curated' checkbox. A 'Save' button is visible. On the right, a table shows the inventory item with its name and a file count of 1. At the bottom, there are buttons for '+ Create', 'Edit', 'Remove', 'Export', and 'JSON'.

4.17.7.7 Org.slf4j-api-1.7.25

<https://mvnrepository.com/artifact/org.slf4j/slf4j-api/1.7.25>

This screenshot shows the 'Occtet Curator' application interface for the project 'org.slf4j-api-1.7.25'. The 'Inventory items' form is displayed, with the 'Inventory name' set to '\slf4j-api-1.7.25-sources.jar' and the 'Software component' set to '\slf4j-api-1.7.25-sources.jar'. The 'Number of files' is 1, and the 'Curated' checkbox is checked. The 'Save' button is present. On the right, a table lists the inventory item with its name and a file count of 1. The bottom of the interface features buttons for '+ Create', 'Edit', 'Remove', 'Export', and 'JSON'.



- Dashboard
- SBOM Mgmt
- Vulnerabilities**
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration

Vulnerabilities

Choose project

org.sif4j:sif4j-api - 1.7.0

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

+ Create

Edit

Remove

Excel

JSON

4.17.7.8 aopalliance -1.0

<https://mvnrepository.com/artifact/aopalliance/aopalliance/1.0>

- Dashboard
- SBOM Mgmt
- Vulnerabilities**
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration

Vulnerabilities

Choose project

aopalliance:aopalliance

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

+ Create

Edit

Remove

Excel

JSON

- Dashboard
- SBOM Mgmt**
- Vulnerabilities
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration

SBOM Mgmt

Choose project

aopalliance:aopalliance - 1

Search files...

0.0

Show all

Files

Overview

Inventory Items

Inventory name

\aopalliance-1.0-sources.jar

Parent inventory item

Software component

\aopalliance-1.0-sources.jar

Download URL

Linking

Priority

Number of files

1

Curated

Created at:

04/20/2026 07:58:13:626

+ Create

Item

Files

\aopalliance-1.0-sources.jar

1

C:\Users\joshah.abah\Documents\Anchor...

0



4.17.7.9 Org-slf4j-api

<https://mvnrepository.com/artifact/org.slf4j/slf4j-api/1.7.36>

The screenshot displays the Occtet Curator web application interface. The left sidebar contains a navigation menu with options: Dashboard, SBOM Mgmt, Vulnerabilities, VEX listing, Projects, Software components, Inventory, Licenses, Copyrights, ORT Issues, ORT Violation, Import, Help, and Administration. The main content area is divided into two sections.

SBOM Mgmt Section:

- Choose project:** org.slf4j:slf4j-api - 1.7.25
- Search files:** Search files... (0/0)
- Show all:** (dropdown)
- Files:** (empty list)
- Overview / Inventory items:**
 - Inventory item:** \slf4j-api-1.7.25-sources.jar
 - Parent inventory item:** (dropdown)
 - Software component:** \slf4j-api-1.7.25-sources.jar
 - Download URL:** (empty field)
 - Linking:** (dropdown)
 - Priority:** (empty field)
 - Number of files:** 1
 - Curated:** (checkbox)
 - Created at:** 04/20/2026 08:02:47:720

Vulnerabilities Section:

- Choose project:** org.slf4j:slf4j-api - 1.7.
- Table headers:** ID, Aliases, Severity, Exploitability, Risk score, Source URL, Manually created, Last update.
- Table body:** (empty)
- Buttons:** + Create, Edit, Remove, Excel, JSON.

4.17.7.10 Commons-collections 3.2.2

<https://mvnrepository.com/artifact/commons-collections/commons-collections/3.2.2>



Octet Curator SBOM Mgmt

Choose project: commons-collections - 3.2.2

Search files... Show all

Files

Inventory name: \commons-collections-3.2.2-sources.jar

Parent inventory item: [dropdown] Software component: \commons-collections-3.2.2-sources.jar

Download URL: [text field]

Linking: [dropdown] Priority: [text field] Number of files: 1 Curated: [checkbox]

Created at: 04/20/2026 07:58:37:431

[curator-admin]

Octet Curator Vulnerabilities

Choose project: commons-collections -

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update

[curator-admin]

+ Create Edit Remove

Excel JSON

4.17.8 Javascript/Typescript projects

4.17.8.1 Tslib-2.8.1

<https://github.com/microsoft/tslib/tree/v2.8.1>

<https://github.com/isaacs/inherits/tree/v2.0.4>

OCCTET Deliverable Number: D 3.3 - SME Toolkit-Demo-Del - page 170



4.17.8.4 Hasown-2.0.2

<https://github.com/inspect-js/hasOwn/tree/v2.0.2>

Octet Curator

SBOM Mgmt

Choose project: **hasOwn - 2.0.2**

Search files... **0.0**

Show all

Files

Inventory Items

Overview **Inventory Items**

C:\Users\joshiah.abah\AppData\Local\Temp\syft-archive-contents-1353267835\hasOwn-2.0.2\github\workflows\node-aught.yml

Inventory Item Vulnerabilities Files Audit notes Licenses Copyrights

Save

Item **0** Files **1**

C:\Users\joshiah.abah\AppData\Local\Temp\syft-archive-contents-1353267835\hasOwn-2.0.2\github\workflows\node-aught.yml

Inventory name

C:\Users\joshiah.abah\AppData\Local\Temp\syft-archive-contents-1353267835\hasOwn-2.0.2\github\workflows\node-aught.yml

Parent inventory item

Software component

C:\Users\joshiah.abah\AppData\Local\Temp\syft-archive-contents-1353267835\hasOwn-2.0.2\github\workflows\node-aught.yml

Download URL

Linking **1** Curated

Created at: 04/21/2026 11:25:49:782

Vulnerabilities

Choose project: **hasOwn - 2.0.2**

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

[curator-admin] **Create** **Edit** **Remove** **Excel** **JSON**

4.17.8.5 Js-tokens-4.0.0

<https://github.com/lydell/js-tokens/tree/v4.0.0>



Octet Curator

SBOM Mgmt

Choose project: js-tokens - 4.0.0

Search files... Show all

Files

Overview **Inventory items**

C:\Users\josiah.abah\AppData\Local\Temp\syft-archive-contents-622904267\js-tokens-4.0.0\package-lock.json

Inventory item: C:\Users\josiah.abah\AppData\Local\Temp\syft-archive-contents-622904267\js-tokens-4.0.0\package-lock.json

Parent inventory item: C:\Users\josiah.abah\AppData\Local\Temp\syft-archive-contents-622904267\js-tokens-4.0.0\package-lock.json

Software component: C:\Users\josiah.abah\AppData\Local\Temp\syft-archive-contents-622904267\js-tokens-4.0.0\package-lock.json

Download URL: NOASSERTION

Linking: Priority: Number of files: 1 Curated

Created at: 04/21/2026 11:27:35:837

Octet Curator

Vulnerabilities

Choose project: js-tokens - 4.0.0

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update

Created at: 04/21/2026 11:28:41:867

4.17.8.6 Safe-buffer-5.2.1

<https://github.com/feross/safe-buffer/tree/v5.2.1>

Octet Curator

SBOM Mgmt

Choose project: safe-buffer - 5.2.1

Search files... Show all

Files

Overview **Inventory items**

C:\Users\josiah.abah\Documents\Anchore-safe-buffer-5.2.1.zip-sha256:1004695c060460e435524ab754d8ad5abf6fcd3c633874c2f5f5c583b2b6e29 (NOASSERTION)

Inventory item: C:\Users\josiah.abah\Documents\Anchore-safe-buffer-5.2.1.zip-sha256:1004695c060460e435524ab754d8ad5abf6fcd3c633874c2f5f5c583b2b6e29 (NOASSERTION)

Parent inventory item: C:\Users\josiah.abah\Documents\Anchore-safe-buffer-5.2.1.zip-sha256:1004695c060460e435524ab754d8ad5abf6fcd3c633874c2f5f5c583b2b6e29 (NOASSERTION)

Software component: C:\Users\josiah.abah\Documents\Anchore-safe-buffer-5.2.1.zip-sha256:1004695c060460e435524ab754d8ad5abf6fcd3c633874c2f5f5c583b2b6e29 (NOASSERTION)

Download URL: NOASSERTION

Linking: Priority: Number of files: 0 Curated

Created at: 04/21/2026 11:28:41:867



4.17.8.8 Has-symbols-1.1.0

<https://github.com/inspect-js/has-symbols/tree/v1.1.0>

4.17.8.9 Wrappy-1.0.20

<https://github.com/isaacs/wrappy/tree/v1.0.2>



Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT issues
ORT Violation
Import
Help
Administration

SBOM Mgmt

Choose project
wrappy - 1.0.2

Search files...

Show all

Files

Overview

Inventory items

C--Users-josiah.abah-Documents-Anchore-wrappy-1.0.2.zip-sha256:13c5eede5d42f00d77ea09c88d7691a02d852fefd9ef4d46a110c715d2a5ef6 (NOASSERTION)

Inventory item

Vulnerabilities

Files

Audit notes

Licenses

Copyrights

Save

Item

Files

Inventory name

C--Users-josiah.abah-Documents-Anchore-wrappy-1.0.2.zip-sha256:13c5eede5d42f00d77ea09c88d7691a02d852fefd9ef4d46a110c715d2a5ef6 (NOASSERTION)

Parent inventory item

Software component

C--Users-josiah.abah-Documents-Anchore-wrappy-1.0.2.zip

Download URL

NOASSERTION

Linking

Priority

Number of files

Curated

Created at

04/21/2026 11:30:23:071

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT issues
ORT Violation
Import
Help
Administration

Vulnerabilities

Choose project
wrappy - 1.0.2

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Manually created	Last update
----	---------	----------	----------------	------------	------------	------------------	-------------

Create

Edit

Remove

Excel

JSON

4.17.9 Eclipse Projects

4.17.9.1 Eclipse-Mosquitto 2.1.2

<https://github.com/eclipse/mosquitto>



https://occtet.bitsea.de/boc/audit-view/204

Octet Curator

SBOM Mgmt

Choose project: **eclipse-mosquitto - test**

Search files... **Show all**

Files

- 1.2.0-id
 - c
 - common
 - constants.c
 - constants.h
 - context.c
 - context.h
 - dictionary.c
 - dictionary.h
 - dictionary_inc.h
 - platform.c
 - platform.h
 - shared_dictionary.c
 - shared_dictionary_internal.h
 - static_init.h
 - transform.c
 - transform.h
 - version.h
 - dec
 - bit_reader.c
 - bit_reader.h
 - decode.c
 - huffman.c
 - huffman.h
 - prefix.c
 - prefix.h

[admin]

Overview

> Copyrights (0)

> Licenses (14)

> Vulnerabilities (0)

Vulnerability	Risk score of vulnerability	Number in software components
---------------	-----------------------------	-------------------------------

Item **Files #**

- > docker.io/eclipse-mosquitto:latest (N...
- lib/apk/ld/install
- usr/bin/mosquitto_ctl
- usr/bin/mosquitto_passwd
- usr/bin/mosquitto_pub
- usr/bin/mosquitto_r1
- usr/bin/mosquitto_signal
- usr/bin/mosquitto_sub
- usr/lib/mosquitto.so.1
- usr/lib/mosquitto_act_file.so
- usr/lib/mosquitto_dynamic_security.so
- usr/lib/mosquitto_password_file.so
- usr/lib/mosquitto_permit_sqli.so
- usr/lib/mosquitto_sparkplug_aware.so
- usr/sbin/mosquitto

https://occtet.bitsea.de/boc/audit-view/204

Octet Curator

SBOM Mgmt

Choose project: **eclipse-mosquitto - test**

Search files... **Show all**

Files

- 1.2.0-id
 - c
 - common
 - constants.c
 - constants.h
 - context.c
 - context.h
 - dictionary.c
 - dictionary.h
 - dictionary_inc.h
 - platform.c
 - platform.h
 - shared_dictionary.c
 - shared_dictionary_internal.h
 - static_init.h
 - transform.c
 - transform.h
 - version.h
 - dec
 - bit_reader.c
 - bit_reader.h
 - decode.c
 - huffman.c
 - huffman.h
 - prefix.c
 - prefix.h

[admin]

Overview

> Copyrights (0)

> Licenses (14)

License	Number in software components
MPL 2.0	2
MIT	9
Apache 2.0	3
BSD-3-Clause	3
BSD-2-Clause	1
GPL 2.0-only	8
CC0-1.0	1
Zlib	1
LOPL 3.0 or later	4

> Vulnerabilities (0)

Item **Files #**

- > docker.io/eclipse-mosquitto:latest (N...
- lib/apk/ld/install
- usr/bin/mosquitto_ctl
- usr/bin/mosquitto_passwd
- usr/bin/mosquitto_pub
- usr/bin/mosquitto_r1
- usr/bin/mosquitto_signal
- usr/bin/mosquitto_sub
- usr/lib/mosquitto.so.1
- usr/lib/mosquitto_act_file.so
- usr/lib/mosquitto_dynamic_security.so
- usr/lib/mosquitto_password_file.so
- usr/lib/mosquitto_permit_sqli.so
- usr/lib/mosquitto_sparkplug_aware.so
- usr/sbin/mosquitto



https://occtet.bitsea.de/boc/vulnerabilities

Octet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities**
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration

Vulnerabilities

Choose project
eclipse-mosquito - te: [Show all](#)

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Last update
----	---------	----------	----------------	------------	------------	-------------

[admin] [Edit](#) [Remove](#) [Excel](#) [JSON](#)

https://occtet.bitsea.de/boc/software-components

Octet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities
- VEX listing
- Projects
- Software components**
- Inventory
- Licenses
- Copyrights
- ORT Issues
- ORT Violation
- Import
- Help
- Administration

Software components

Choose project
eclipse-mosquito - te: [Show all](#)

> Filter

50 rows

Name	Version	PURL	Licenses	Curated	License controlled by AI
alpine-base	3.7.1-r0	pkg:apk/alpine/alpine-base@3.7.1-r0?arch=r8s...	GPL-2.0-only	False	
alpine-base-layout	3.7.1-r0	pkg:apk/alpine/alpine-base-layout@3.7.1-r0?arch...	GPL-2.0-only	False	
alpine-keys	2.6-r0	pkg:apk/alpine/alpine-keys@2.6-r0?arch=r8s,64ddist...	MIT	False	
alpine-release	3.23.3-r0	pkg:apk/alpine/alpine-release@3.23.3-r0?arch=r8s,6...	MIT	False	
apk-tools	3.0.3-r1	pkg:apk/alpine/apk-tools@3.0.3-r1?arch=r8s,64ddist...	GPL-2.0-only	False	
argon2-libs	20190702-r5	pkg:apk/alpine/argon2-libs@20190702-r5?arch=r8s,6...	Apache-2.0, CC0-1.0	False	
broto-libs	1.2.0-r0	pkg:apk/alpine/broto-libs@1.2.0-r0?arch=r8s,64ddist...	MIT	False	
busybox	1.37.0-r30	pkg:apk/alpine/busybox@1.37.0-r30?arch=r8s,64ddist...	GPL-2.0-only	False	
busybox-binsh	1.37.0-r30	pkg:apk/alpine/busybox-binsh@1.37.0-r30?arch=r8s...	GPL-2.0-only	False	
ca-certificates	20251003-r0	pkg:apk/alpine/ca-certificates@20251003-r0?arch=r8...	MIT, MPL-2.0	False	True
ca-certificates-bundle	20251003-r0	pkg:apk/alpine/ca-certificates-bundle@20251003-r0...	MPL-2.0, MIT	False	True
cjson	1.7.19-r1	pkg:apk/alpine/cjson@1.7.19-r1?arch=r8s,64ddist...	MIT	False	
gmp	6.3.0-r4	pkg:apk/alpine/gmp@6.3.0-r4?arch=r8s,64ddist...	LGPL-3.0-or-later, GPL-2.0-or-later	False	
gnutls	3.8.11-r0	pkg:apk/alpine/gnutls@3.8.11-r0?arch=r8s,64ddist...	LGPL-2.1-or-later	False	
libapk	3.0.3-r1	pkg:apk/alpine/libapk@3.0.3-r1?arch=r8s,64ddist...	GPL-2.0-only	False	
libcrypto3	3.5.5-r0	pkg:apk/alpine/libcrypto3@3.5.5-r0?arch=r8s,64ddis...	Apache-2.0	False	
libedit	20251016.3.1-r0	pkg:apk/alpine/libedit@20251016.3.1-r0?arch=r8s,64...	BSD-3-Clause	False	
libffi	3.5.2-r0	pkg:apk/alpine/libffi@3.5.2-r0?arch=r8s,64ddist...	MIT	False	
libidn2	2.3.8-r0	pkg:apk/alpine/libidn2@2.3.8-r0?arch=r8s,64ddist...	GPL-2.0-or-later, LGPL-3.0-or-later	False	
libmicrohttpd	1.0.2-r1	pkg:apk/alpine/libmicrohttpd@1.0.2-r1?arch=r8s,64s...	LGPL-2.1-or-later	False	
libcurl	6.5.0-20251123-r0	pkg:apk/alpine/libcurl@6.5.0-20251123-r0?arch...	X11	False	
libssl3	3.5.5-r0	pkg:apk/alpine/libssl3@3.5.5-r0?arch=r8s,64ddist...	Apache-2.0	False	
libtasn1	4.19.0-r0	pkg:apk/alpine/libtasn1@4.19.0-r0?arch=r8s,64ddis...	LGPL-2.1-or-later	False	

[admin] [Create](#) [Edit](#) [Remove](#)

4.17.9.2 Hadoop 3.4.1

<https://github.com/apache/hadoop>



https://occtet.bitsea.de/boc/audit-view/203

Octet Curator

- Dashboard
- SBOM Mgmt**
- Vulnerabilities
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ! ORT Issues
- ! ORT Violation
- Import
- Help
- Administration

SBOM Mgmt

Choose project: **hadoop - test**

Search files...

Show all

Files

Overview

- Copyrights (3)
- Licenses (8)
- Vulnerabilities (239)**

Vulnerability	Risk score of vulnerability	Number in software components
VCID-99th-4w2u-aaaa	3.4	1
VCID-8z3f-pes5-aaag	3.5	1
VCID-4kxv-uyf1-aaag	4.5	3
VCID-22zb-14rc-aaam	4.5	1
VCID-wu2q-msat-ckay	3.1	1
VCID-52ah-igav-aaad	4.5	1
VCID-18ar-u5pe-aaag	3.1	14
VCID-7ffu-u2bq-bogw	4	11
VCID-qfmr-vnce-97ag	4	3

[admin]

https://occtet.bitsea.de/boc/vulnerabilities

Octet Curator

- Dashboard
- SBOM Mgmt
- Vulnerabilities**
- VEX listing
- Projects
- Software components
- Inventory
- Licenses
- Copyrights
- ! ORT Issues
- ! ORT Violation
- Import
- Help
- Administration

Vulnerabilities

Choose project: **hadoop - test** Show all

Filter

ID	Aliases	Severity	Exploitability	Risk score	Source URL	Last update
VCID-1thy-wz44-53f6	CVE-2025-52099, GHSA-H4dc-H4q4-95D	8	0.5	4	http://public.vulnabr.ecode.io/vulnerabilities/VCID-1thy-wz44-53f6	04/07/2026 08:57:56:470
VCID-amtp-3a67-7f9w	CVE-2025-49128, GHSA-wf8F-6423-qfng	6.2	0.5	3.1	http://public.vulnabr.ecode.io/vulnerabilities/VCID-amtp-3a67-7f9w	04/07/2026 08:57:56:614
VCID-qf68-b7ap-hyc7	GHSA-729v-8253-57eq	8	0.5	4	http://public.vulnabr.ecode.io/vulnerabilities/VCID-qf68-b7ap-hyc7	04/07/2026 08:57:56:675
VCID-213j-gkio-aaab	CVE-2023-35116	6.8	0.5	3.4	http://public.vulnabr.ecode.io/vulnerabilities/VCID-213j-gkio-aaab	04/07/2026 08:57:57:956
VCID-29yb-b7ro-aaag	CVE-2020-36318, GHSA-513z-w4Cz-62b2	8	0.5	4	http://public.vulnabr.ecode.io/vulnerabilities/VCID-29yb-b7ro-aaag	04/07/2026 08:57:57:940
VCID-trmk-w8wv-aaar	CVE-2021-44877, GHSA-3a7a-79m2-3w2w	8	0.5	4	http://public.vulnabr.ecode.io/vulnerabilities/VCID-trmk-w8wv-aaar	04/07/2026 08:57:58:006
VCID-k3ks-dhsh-aaah	CVE-2020-25549, GHSA-28bc-cy4e-88qj	8	0.5	4	http://public.vulnabr.ecode.io/vulnerabilities/VCID-k3ks-dhsh-aaah	04/07/2026 08:57:58:144
VCID-174k-g3ln-aaan	CVE-2022-42003, GHSA-4j3h-3j3p-w8ff	8	0.5	4	http://public.vulnabr.ecode.io/vulnerabilities/VCID-174k-g3ln-aaan	04/07/2026 08:57:58:225
VCID-tr9w-v8r2-27f6	CVE-2025-48734, GHSA-wu15-973w-8w9f	8	0.5	4	http://public.vulnabr.ecode.io/vulnerabilities/VCID-tr9w-v8r2-27f6	04/07/2026 08:58:02:554
VCID-y18g-fefm-aaar	CVE-2023-4586, GHSA-57m3-F3y5-hm5m	6.7	0.5	3.4	http://public.vulnabr.ecode.io/vulnerabilities/VCID-y18g-fefm-aaar	04/07/2026 08:58:06:558
VCID-qy5c-3c7a-aaak	CVE-2022-48152, GHSA-5b7m-mt4q-vm4	6.8	0.5	3.4	http://public.vulnabr.ecode.io/vulnerabilities/VCID-qy5c-3c7a-aaak	04/07/2026 08:58:06:756
VCID-z2kh-59ks-aaac	CVE-2021-37136, GHSA-gr4k-wr2h-rf9v	9	0.5	4.5	http://public.vulnabr.ecode.io/vulnerabilities/VCID-z2kh-59ks-aaac	04/07/2026 08:58:06:423
VCID-39a8-1b77-aaac	CVE-2019-16869, GHSA-p979-4m3w-53vg	9	0.5	4.5	http://public.vulnabr.ecode.io/vulnerabilities/VCID-39a8-1b77-aaac	04/07/2026 08:58:06:290
VCID-up5w-v1f8-qgq7	CVE-2025-58057, GHSA-36dm-j85a-pgmj	6.8	0.5	3.4	http://public.vulnabr.ecode.io/vulnerabilities/VCID-up5w-v1f8-qgq7	04/07/2026 08:58:07:069
VCID-jm8g-z3vs-wqcm	CVE-2025-58056, GHSA-1g9v-69hy-q649	6.8	0.5	3.4	http://public.vulnabr.ecode.io/vulnerabilities/VCID-jm8g-z3vs-wqcm	04/07/2026 08:58:07:972
VCID-mjpf-8s0z-aaag	CVE-2024-29025, GHSA-5gpm-x58v-624v	6.3	0.5	3.1	http://public.vulnabr.ecode.io/vulnerabilities/VCID-mjpf-8s0z-aaag	04/07/2026 08:58:08:044
VCID-a2b6-91uk-hqbg	CVE-2024-47335, GHSA-xq3w-v528-46rv	8	0.5	4	http://public.vulnabr.ecode.io/vulnerabilities/VCID-a2b6-91uk-hqbg	04/07/2026 08:58:10:410
VCID-mc7g-j4n5-aaaf	CVE-2022-40161, GHSA-hw4q-5f5g-f92x	6.2	0.5	3.1	http://public.vulnabr.ecode.io/vulnerabilities/VCID-mc7g-j4n5-aaaf	04/07/2026 08:58:10:477
VCID-k8mm-82b2-7b7g	CVE-2025-25193, GHSA-389v-839f-4b7x	6.2	0.5	3.1	http://public.vulnabr.ecode.io/vulnerabilities/VCID-k8mm-82b2-7b7g	04/07/2026 08:58:10:477
VCID-awbw-f32z-53hz	CVE-2025-24970, GHSA-493c-wm8a-jfw	8	0.5	4	http://public.vulnabr.ecode.io/vulnerabilities/VCID-awbw-f32z-53hz	04/07/2026 08:58:11:126
VCID-dyp4-hwud-v7cu	CVE-2024-47361, GHSA-r79p-v2c8-mf93	9	0.5	4.5	http://public.vulnabr.ecode.io/vulnerabilities/VCID-dyp4-hwud-v7cu	04/07/2026 08:58:20:548
VCID-jh64-y89v-aaah	CVE-2023-39410, GHSA-nrvv-645h-jfh, PYSEC-0000-CVE-2023-39410, PYSEC-2023-188	9	0.5	4.5	http://public.vulnabr.ecode.io/vulnerabilities/VCID-jh64-y89v-aaah	04/07/2026 08:58:20:623
VCID-2p9q-7b21-mkfu	CVE-2025-68161, GHSA-vc5p-v89e-52mj	6.2	0.5	3.1	http://public.vulnabr.ecode.io/vulnerabilities/VCID-2p9q-7b21-mkfu	04/07/2026 08:58:42:354
VCID-d2zr-c25i-aaai	CVE-2024-41909, GHSA-222b-hv7a-3m9f	8	0.5	4	http://public.vulnabr.ecode.io/vulnerabilities/VCID-d2zr-c25i-aaai	04/07/2026 08:58:46:651

[admin]

Edit Remove

Excel JSON



https://occtet.bitsea.de/boc/software-components

Octet Curator

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT Issues
ORT Violation
Import
Help
Administration

Software components

Choose project
hadoop - test
Show all

Filter

Name	Version	PURL	Licenses	Curated	License controlled by AI
ant		pkg:maven/org.apache.ant/ant		False	
ant-junit		pkg:maven/org.apache.ant/ant-junit		False	
commons-lang3	3.4	pkg:maven/org.apache.commons/commons-lang3@3.4		False	
commons-collections4		pkg:maven/org.apache.commons/commons-collections4		False	
commons-compress		pkg:maven/org.apache.commons/commons-compress		False	
commons-crypto		pkg:maven/org.apache.commons/commons-crypto		False	
commons-csv		pkg:maven/org.apache.commons/commons-csv		False	
commons-dbc2	2.1.1	pkg:maven/org.apache.commons/commons-dbc2@2.1.1		False	
commons-dbc2	2.12.0	pkg:maven/org.apache.commons/commons-dbc2@2.12.0		False	
commons-jstl	2.1.1	pkg:maven/org.apache.commons/commons-jstl@2.1.1		False	
commons-lang3		pkg:maven/org.apache.commons/commons-lang3		False	
commons-lang3	3.14.0	pkg:maven/org.apache.commons/commons-lang3@3.14.0		False	
commons-lang3	3.7	pkg:maven/org.apache.commons/commons-lang3@3.7		False	
commons-lang3	3.8	pkg:maven/org.apache.commons/commons-lang3@3.8		False	
commons-lang3	3.8.1	pkg:maven/org.apache.commons/commons-lang3@3.8.1		False	
commons-lang3	3.9	pkg:maven/org.apache.commons/commons-lang3@3.9		False	
commons-math		pkg:maven/org.apache.commons/commons-math		False	
commons-math3		pkg:maven/org.apache.commons/commons-math3		False	
commons-pool2		pkg:maven/org.apache.commons/commons-pool2		False	
commons-pool2	2.12.0	pkg:maven/org.apache.commons/commons-pool2@2.12.0		False	
commons-rng-simple	1.4	pkg:maven/org.apache.commons/commons-rng-simple@1.4		False	
commons-text		pkg:maven/org.apache.commons/commons-text		False	

[admin] + Create Edit Remove

https://occtet.bitsea.de/boc/audit-view/203

Octet Curator

Dashboard
SBOM Mgmt
Vulnerabilities
VEX listing
Projects
Software components
Inventory
Licenses
Copyrights
ORT Issues
ORT Violation
Import
Help
Administration

SBOM Mgmt

Choose project
hadoop - test
Search files...
Show all

Files

Overview Inventory items

03dd7428-d188-480e-afde-56acce9cac25 (NOASSERTION) x 00bc973e-f93e-495d-9e19-28601eb2650a9.4.53 v20231009 (NOASSERTION) x

Inventory item Vulnerabilities Files Audit notes Licenses Copyrights

Save

Filter

Resolved	ID	Aliases	Severity	Exploitability	Risk score
☒	VDB-jax7-qcuf-zyer	CVE-2024-13009, GHSA-q4v-gq96-w7c5	8	0.5	4
☒	VDB-84db-qrs3-7tpg	CVE-2024-8184, GHSA-g8m5-722b-bwhq	6.2	0.5	3.1

Update vulnerabilities Create VEX

Item Files

00bc973e-f93e-495d-9e19-28601eb2650a9.4.53	0	0	0
01800b0e-12a2-43bf-bdaf-993028...	0	0	0
0221409c-e0c5-4904-a0f7-68904c...	0	0	0
025e9952-9384-42b0-87c1-c5c55...	0	0	0
02c37190-63f9-41a9-9406-f9f089b...	0	0	0
03c39ae1-c044-4d11-94f3-02af57...	0	0	0
03d87428-d188-480e-afde-56acce...	0	0	0
03d8c3b4-4990-4370-adc6-d1440...	0	0	0
03d8f673-7789-48e7-959a-637f85...	0	0	0
03d76744-18c3-403c-8096-639f11...	0	0	0
04069907-678e-4884-925c-c2c77...	0	0	0
04744905-063e-44e3-b133-d3e6d...	0	0	0
04789f6b-1660-4258-8c33-f22460...	0	0	0
04970c7e-503f-49e0-9f62-4cc367...	0	0	0
04d13ac9-a35a-4348-9b72-47619f...	0	0	0
050a84c6-3121-4183-9805-709a0...	0	0	0
05685451-409c-4138-b000-26864...	0	0	0
05904770-537e-4995-9442-607f0...	0	0	0
05a295f7-980c-43f9-8a0b-6496d...	0	0	0
06d55581-6a16-466a-bc5b-17166...	0	0	0
06a632a0-7659-4595-09e5-0f02b...	0	0	0
06a670c7-432e-4c08-b040-5b0e8...	0	0	0
0728641e-9f56-4696-094c-63e6f5...	0	0	0
082b2277-9996-43d5-9683-c19c7...	0	0	0
08d0133a-9564-44cc-9561-f828d...	0	0	0
0946ec93-54c3-4208-a13c-56c7b...	0	0	0
0950ff9f-64fa-40d0-a016-3a69d...	0	0	0
0b02c8ff-c704-4351-a8a3-7415c...	0	0	0
0c358643-c5af-4dc5-940c-90329f4...	0	0	0

4.18 Conclusion

The functionality of the curator tool is comprehensive, significantly streamlining the security and compliance workflow for software components. Specifically, it enables the acquisition of Software Component Test Data, referred to as SME test data, by scanning the ORT Server.



This scanning capability ensures that the most current security posture and dependency information are retrieved directly from the source.

Once the data is retrieved, the curator provides a robust environment for security professionals to actively work on identifying, prioritizing, and resolving discovered security issues or vulnerabilities. This includes a detailed interface for issue management and remediation tracking.

A critical feature of the curator is its ability to generate a Vulnerability Exploitability eXchange (VEX) document when necessary. The VEX, a structured data format, allows organizations to communicate which discovered vulnerabilities are actually exploitable or pose a risk within the specific context of their software product, thereby reducing alert fatigue and focusing remediation efforts on true threats.

Finally, the entire process—including the acquired SME test data, the managed issues, and the created VEX document—can be successfully exported into a standardized Software Bill of Materials (SBOM) format. This export functionality applies equally well to the SME Test Data as it does to the analysis performed on the aforementioned 'iconic projects'. This ensures compliance, facilitates secure supply chain management, and provides a clear, auditable record of the security status of all analyzed components.



5 Conclusions

The OCCTET toolkit demonstrator provides a comprehensive functionality that significantly streamlines the security and compliance workflow for software components. By directly integrating the Curator with the ORT Server, the system ensures that the most current dependency and security posture information is successfully retrieved and analyzed, as evidenced by the processing of Small and Medium-sized Enterprise (SME) test data. This integration delivers a robust environment for security professionals to actively identify, prioritize, track, and resolve discovered security issues and vulnerabilities.

Testing the ORT Server against prominent open-source projects demonstrated significant analytical depth. While certain limitations were identified during the testing phase such as processing errors with specific NPM projects and an ongoing lack of support for GitHub Actions the ORT Server generally captures a more complete dependency picture than standard repository security tools. Notably, it effectively identifies compatible Python dependencies and non-standard Maven scopes, and accurately distinguishes between distributed product components and build-time dependencies (e.g., Maven plugins). For ecosystems lacking dedicated package managers, such as C/C++, the system ensures continued traceability by providing fallback mechanisms to manually declare dependencies in machine-readable formats like SPDX.

A critical capability of the toolchain is the generation of Vulnerability Exploitability eXchange (VEX) documents. This structured data format allows organizations to communicate the true exploitability of specific vulnerabilities within the context of their software, thereby reducing alert fatigue and focusing remediation efforts on actual threats. Ultimately, the entire curated analysis, encompassing acquired test data, managed vulnerabilities, and generated VEX documentation, can be exported into standardized Software Bill of Materials (SBOM) formats. Validated across both SME data and iconic open-source projects, these exports ensure regulatory compliance, facilitate secure supply chain management, and provide a clear, auditable record of the security status of all integrated components.



6 ACRONYMS AND ABBREVIATION

CRA — Cyber Resilience Act
ENISA — European Union Agency for Cybersecurity
EU — European Union
GDPR — General Data Protection Regulation
FOSS — Free and Open-Source Software
AI — Artificial Intelligence
IPR — Intellectual Property Rights
KPI — Key Performance Indicator
PII — Personally Identifiable Information
RBAC — Role-Based Access Control
SBOM — Software Bill of Materials
SAST — Static Application Security Testing
DAST — Dynamic Application Security Testing
MFA — Multi-Factor Authentication
SOC — Security Operations Centre
IR — Incident Response
API — Application Programming Interface
TLS — Transport Layer Security
ISO — International Organization for Standardization
IEC — International Electrotechnical Commission
ETSI — European Telecommunications Standards Institute
SUS — System Usability Scale
TRL — Technology Readiness Level
WP — Work Package
DoA — Description of Action



7 BIBLIOGRAPHY

1. **Regulation (EU) 2024/2847 of the European Parliament and of the Council** of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), Official Journal of the European Union, L, 2024.
2. **European Union Agency for Cybersecurity (ENISA)**, Good Practices for Security of Products with Digital Elements, ENISA, 2023.
3. **European Union Agency for Cybersecurity (ENISA)**, Guidelines for Coordinated Vulnerability Disclosure, ENISA, 2022.
4. **ISO/IEC 27001:2022**, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, International Organization for Standardization / International Electrotechnical Commission, Geneva.
5. **ISO/IEC 62443-4-1:2018**, Security for industrial automation and control systems — Secure product development lifecycle requirements, ISO/IEC.
6. **ETSI EN 303 645 V2.1.1** (2020), Cyber Security for Consumer Internet of Things: Baseline Requirements, European Telecommunications Standards Institute.
7. **Directive (EU) 2022/2555** (NIS2 Directive) of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, Official Journal of the European Union, L 333, 27.12.2022.
8. **European Commission**, The Cyber Resilience Act — Questions & Answers, European Commission, 2024.
9. **European Commission**, DIGITAL Europe Programme – Model Grant Agreement, European Commission, 2024.
10. **OCCTET Project Consortium**, Description of Action (DoA), Grant Agreement No. 101190474, 2024.
11. **OCCTET Project Consortium**, CRA SME requirements and self-assessment checklists (D1.2), 2025.
12. **Technical Guideline TR-03183** "Cyber Resilience Requirements." Software bills of materials (SBOMs) are among the key requirements of the European Cyber Resilience Act (CRA). Software bills of materials (SBOMs) are among the key requirements of the European Cyber Resilience Act (CRA).

Note: All regulatory and standards references correspond to the versions in force at the time of deliverable submission (March 2026).