

# **CAST SBOM Manager** Installation & User Guide

Version: 2.0.0 Date: July, 2024

# Contents

ntroduction	4
Pre-requisites	4
Overview of the Process	5
I. Installation	5
Windows installation	5
Linux installation	6
2. Application Initialization	7
3. Creating a SBOM	9
Step 1 – Details	9
Step 2 – Files	.10
Step 3 – Packages	.11
Step 4 – Scanners	.12
Step 5 – Summary	.13
4. Browsing and Editing a SBOM	.14
Home Screen	.14
Projects	.15
Bill of Materials	.16
Dashboards	.17
Components	.18
File Map	.20
SBOM Export	.21
Catalog	.22

### CAST SBOM Manager

Component Categories	.23
Propagate component changes in SBOMs	.25
Find component usage across SBOMs	.25
Licenses	.26
Create/Edit a license	.27
Create/Edit a license policy	.29
Vulnerabilities	.31
Edit a vulnerability	.33
Find vulnerable SBOMs	.34
Log a vulnerability	.35
Preferences & Configuration	.36

# Introduction

CAST SBOM Manager is a complementary product to CAST Highlight dedicated to Software Composition Analysis (SCA) and Bill of Materials (SBOM) management. This new product is designed to facilitate the following use cases:

1. Enhance SBOM reviews and documentation by recording user modifications (e.g., choice of a license for a dual-licensed component, internal component reviews, etc.) and retrieving this metadata for future SBOMs.

2. Cataloguing and identification of proprietary components (i.e., developed in house) to automatically detect them along with their metadata (custom licenses, copyright information, etc.) in future SBOMs.

### **Pre-requisites**

CAST SBOM Manager has the following pre-requisites. Please ensure your machine meets these requirements prior to installing and running the product.

- Internet Access: Since the product interacts with CAST Highlight's SCA database, the machine where the product will be running requires access to the Internet.
- Operating System: Windows (10 preferred), Linux
- Java Runtime Environment: JRE 11 (required for Linux)
- Local Port 9001 should be available
- RAM/Memory: 16GB recommended
- Storage Drive Space: 200MB minimum

# C/ST

# **Overview of the Process**

Following is a general overview of each major step in the process for using the SBOM Manager:

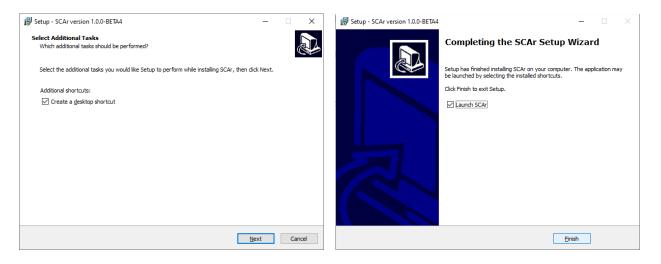
- 1. Installation
- 2. Application Initialization
- 3. Creating a SBOM
- 4. Browsing and editing a SBOM

# 1. Installation

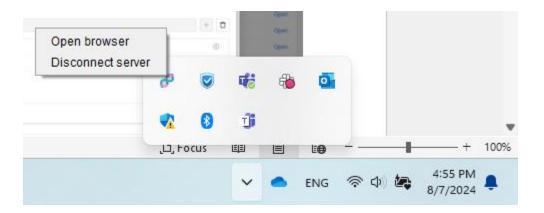
### Windows installation

To install the SBOM Manager, simply follow the steps below:

- Execute the installer .exe (e.g., sbom-manager-2.0.0-RC4-setup.exe)
- Select your preferred language and other preferences for the installation



 Once the installation is finished, a browser automatically opens the application for the initialization step. If the browser doesn't open automatically, go directly to http://localhost:9001  If the browser doesn't open automatically, open the system tray icons, right click on the SBOM Maanger icon and click on "Open browser"



- By default, the application uses port 9001. If there is an issue, first check for a
  possible conflict on this port from another application running on the machine.
- If this port is already in use by another application, you can change it by following these steps (under Windows):
  - locate the sbom-manager.exe folder location (generally %USER%\AppData\Local\Programs\sbom-manager\)
  - o create a file called sbom-manager.l4j.ini next to sbom-manager.exe
  - Add into it the line: -Dserver.port=9091 (choose the port you prefer)

### Linux installation

- Download the SBOM installation ZIP file
- Ensure GUI/XDRP is installed/enabled
- Run the following commands
  - o unzip sbom-manager-2.0.0-RC3-linux.zip -d sbom-manager-2.0.0-RC3-linux
  - o cd sbom-manager-2.0.0-RC3-linux/bin
  - o chmod 755 \* ## make sure sbom-manager.sh have execute permission
  - o ./sbom-manager.sh ##will launch the sbom manager process

- ps -ef|grep som ##check if process(/usr/bin/java -Xms2048m -Xmx8192m -jar /home/hluser/sbom-manager-2.0.0-RC3-linux/bin/../lib/sbom-manager.jar) running
- o netstat -plten|grep 9001 ##process is running on 9001 port
- Open the browser and type in <a href="https://localhost:9001">https://localhost:9001</a>

# 2. Application Initialization

Ø	Configuration	Scanner System			+ New BOM	2 0
硷						
₽	* Usage :	Desktop 🗸	Sign in on SCA	Sign Up Sign In 🗙		
ыç	* First name :		Login :	muller974@gmail.com		
E	* Last name :		* Password:	····· Ø		
Ö	* Email :					
\$	Save	Register		Cancel Sign In		
						_

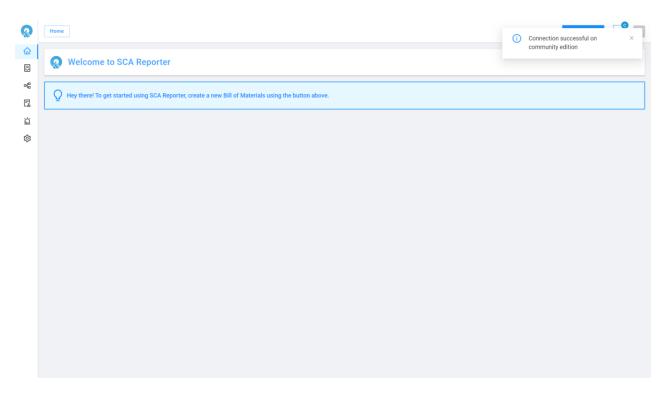
To initialize the application and set up your user account, provide the following information:

- First name and last name: this information remains local to your machine.
- E-mail address: This should be a valid professional e-mail address.
- Password: Define your password that will be associated with your e-mail address to sign in.



SCAr (JavaFX version 8.0.221)			-	×
	🗧 🗲 🔿 🖷 SCAr/Initializ	ation		
				 _
	SCAr Initialization	Sign Up Sign In		
	SCAr Initialization	Sign Op Sign In		
	• Usage mode :	Use your Browser 🗸 🗸		
	* First name :	Michael		
	* Last name :	MULLER		
	* Email :	m.muller@castsoftware.com		
	* Password:			
	* Confirm password	Ø Ø		
		~ •		
		Save		

Once you click on "Save", the screen closes and automatically launches the application after a couple seconds.



# 3. Creating a SBOM

To create a SBOM, click on the "+ New SBOM" button on top right of the screen. A wizard opens to let you specify required information and options.

	BOM Creation			×	
We	1 Details	Name your Bill of Ma	terials		
Q Неу	<ul> <li>Files</li> <li>Packages</li> </ul>	* Product: * Project:	MyCustomApp API		
	4 Scanners 5 Summary	* Version :			
		Chose your license p	olicy		
		+ License policy:	My Policy GPL v3 compliance ASL 3rd party compliance My Policy My Policy	~	
		The following steps	will guide you through the process of creating a new Bill of Materials. This help panel provides additional guidance/context for each of these steps.		
	Cancel			Next	

### Step 1 – Details

Provide product, project, and version names.

Choose the license policy you want to apply for this SBOM. See how to create/edit a license policy later in this document.

Click on "Next" to go to the next step.

ର	Home	New E	Bill of Materials		×	вом
	Ø 1	Ξ	Details	Select the codebase to scan		
20 []_1	Total BC	- == - ()	Source Packages Scanners	Source:      Root codebase folder from local filesystem     CAST Highlight CSV zip archive     Root folder:      Select a Folder	Select	
ت ه	Latest	-	Summary	Add file filters File filter type: Exclude  V		ation   by Update
	CRM > CRM > MyProdu			Select a property V Select a condition V	+ 0	Open Open Open
	Portal CRM >			Eile path is like <u>%tests%</u>	×	Open
				Add file filter exceptions	0	open
				File modified         V         before         V         2022-05-01 21:08:56	8 + 0	
		Can	cel	Pro	evious Next	

### Step 2 – Files

Specify the root folder where source code of the application is located on your machine.

From this step, you can also specify file exclusion or inclusion rules, based on:

- File name
- File path
- File size
- File modified date

File name and path filters use standard Shellscript pattern matching:

- Multiple patterns can be separated by semi-colons
- \* matches 0 or more characters
- ? matches precisely one character
- [!abcABC] matches any character except a,b,c and their uppercase counterparts

Alternatively, you can specify a result .zip file produced by CAST Highlight's agent which contains result CSV files for an application already analyzed by CAST Highlight.

ଛ	Home	BOM Creation		×	ом	
	Home We	~	Package scanner configuration         Enable Maven scanner:         Scan specific POM file:         POM path:       Enter relative path to POM file, eg. /my6ubFolder/pom.xml         Use local maven repository:	×		
			<ul> <li>By enabling the Maven Scanner, SCAr will analyse your POM file and add corresponding Components.</li> <li>By default, the POM file at the project root will be analysed. However, you may chose to scan a specific POM file instead by providing its relative path.</li> <li>Additionally, you may chose to allow the scanner to access your local Maven repository (the location of which is set in the configuration page) in order to facilitate dependency version information retrieval.</li> </ul>			
		Cancel	Previous	Next		

### Step 3 – Packages

For Maven-based applications, you can enable the Maven scanner which will detect components referenced in your pom.xml.

By enabling the Maven Scanner, the SCAR SBOM Manager will analyze your POM file and add corresponding Components.

- By default, the POM file at the project root will be analyzed. However, you may choose to scan a specific POM file instead by providing its relative path.
- Additionally, you may choose to allow the scanner to access your local Maven repository (the location of which is set in the configuration page) to facilitate dependency version information retrieval.



### Step 4 – Scanners

ନ୍ଦ	Home			+ New E	BOM Ø
	Crm > API	BOM Creation	Select scanners to apply Use previous version:	U Dy Cre	eation   by Update Open Open
			In this step you can select the scanners to use for Component matching. These are executed in the order presented until a match is found. • User Components found in a specified previous 800M • Components registered in the SMO Catalog • Components found using the SCA platform. Either simply distinguish between Found/Not Found ( <u>Only known</u> ), match only trusted Components (eg. over 500 stars) in order to limit false positives ( <u>Filtered result</u> ) or perform a <u>Full scan</u> without filtering.		
		Cancel	Previous	Next	

In this step you can select the scanners to use for Component matching. These are executed in the order presented until a match is found.

- Use previous version: Scans for components included in a specified previous SBOM (select the desired version in the "Previous Version" field)
- Use local catalog: Scans for components already existing from previous scans and registered manually in the SBOM Catalog previously
- Use SCA: Scans for components in the CAST Highlight component knowledgebase and allows user to set a filter option:
  - Only known: this mode will let you know whether scanned files are known vs. not known in CAST's SCA knowledgebase
  - Filtered Result: this mode will retain component identifications that correspond to specific filters (e.g., at least 500 stars, exclusion of file fingerprints below 100 bytes, etc.) to reduce noise
  - Full scan: all file fingerprints will be processed for component identification, without any filter



### Step 5 – Summary

From this step, review the configuration that was set up for the scan. To change it, you can go back to previous steps by clicking on the "Previous" button at the bottom of the screen.

୍ଭ	Home					New BOM
<u>۵</u>		BOM Creation			×	
	😡 Weld	Details	Bill of Materials Summary			
ol <mark>0</mark>	Total BOMs	Files	Details			
		Packages		Portal > SpringBoot > 2.5.6		
Ó		Scanners	License policy	My Policy		_
ø	Latest BOMS	5 Summary	Files			by Creation   by Update
	Portal > Spr		Packages	C:\Users\mmu\Documents\hl\$368		
	CRM > API		Enable Maven scanner	R		Open
			Scanners			open.
			Use previous version			
			Use local catalog			
			Use SCA	V Only known		
			Please verify that the information	n provided is correct before launching the <b>Bill of Materials creation process</b> .		
		Cancel			Previous Done	

# 4. Browsing and Editing a SBOM

The sections below detail the primary product capabilities.

### Home Screen

From the homepage, you can retrieve the key information for your SBOMs:

- Total SBOMs created
- Total licenses detected in SBOMs
- Total license policies available
- Total vulnerabilities detected in SBOMs
- A list of recent SBOMs for quick access to a specific SBOM

			+ New BOM	8 <sup>0</sup> 0
come to SCA Reporter				
	Total Licenses	Total Policies	Total Vulnerabilities 🛕 3	
5			by Creation   t	by Update
AST > 1.3.0				Open
ore > 1.1.0				Open
ore > 1.0.1-beta				Open
	AST > 1.3.0 ore > 1.1.0	Total Licenses Total Licenses Total Licenses 129 S S AST > 1.3.0 ore > 1.1.0	Total Licenses ☐ 129 S AST > 1.3.0 ore > 1.1.0	Total Licenses ☐ 129 Total Policies ☐ 4 Total Vulnerabilities ☆ 3 by Creation   1 AST > 1.3.0 ore > 1.1.0 Total Policies ☐ 4 Total Vulnerabilities ☆ 3



### Projects

In this "Projects" view, you can retrieve all the SBOMs which have been created, organized as a tree with the following structure:

- Product
  - Project
    - Version

This structure allows users to organize SBOMs in a flexible way. For instance, a product can be an application and a project can be a specific component of an application.

Clicking on a specific project will display the list of versions with corresponding SBOMs available along with some high-level metrics such as the number of scanned files, number of third-party components detected, number of distinct licenses, and date of creation/update.

BOMs > Projects >	Versions			+ New B	DM 8 2 2
H MyCRM > Core					
Version 👙	Files ¢	Components 💠	Licenses	Updated 💠	
1.1.0	3104	271	26 23/04/2021 09:25:38 +0200		<b>ū</b> 📀
1.0.1-beta	2221	206	24 12/01/2021 14:39:16 +0100	03/06/2021 10:59:16 +0200	Ū 🕑

You can customize this view by showing/hiding some columns of the table. To do so, click on the column icon on top right of the table and configure the columns.

able column preferences			Х
Files		Version	$\equiv$
Vulnerabilities		Licenses	=
		Created	=
	>	Updated	$\equiv$
	<	Components	$\equiv$
Cancel		Reset to defaults	Save

You can also delete a SBOM by clicking on the red trash icon. Finally, you can open the SBOM by clicking on the blue arrow in the last column.

### **Bill of Materials**

In CAST Highlight's SCAR SBOM Manager, the bill of materials is the central place from which you can see and manipulate scan results with regards to components, license policies, obsolescence, and vulnerabilities.



#### Dashboards

Q	BOM         >         Dashboard         Components         File Map		+ New BOM
습 ∃	MyCRM > Core > 1.0.1-beta		License policy: My Policy Export BOM
29 12 13	Created: 12 January 2021, 14:39:16 Updated: 03 June 2021, 10:59:16	Components Files P 206 Files 2,221	Licenses Vulnerabilities     24
ŝ	Files by Source	Components by Category	Components by Obsolescence
	2007 0 5 209 Local Previous Catalog SCA	Proprietary     0       Open Source     204       Sandbox     1       Excluded     0       Undefined     1	Outdated - 40           High - 9           Medium - 85           Up to date - 19           Unknown - 5
	Components by Compliance	Components by Vulnerability	Top 10 Components Licenses 240/266
	160 68 36 2 2 10 10 10 10 10 10 10 10 10 10	0 0 0 0	Apache-2.0 119 path-exception 24 EPL-2.0 20 MIT 18 BSD-Family 14 OASSERTION 13 CCO-1.0 12 BSD-2-Clusse 7 W3C 7

This page summarizes the different KPIs and metrics of a SBOM:

- Create and update dates
- Number of components detected
- Number of files scanned
- Number of licenses detected
- Number of vulnerabilities detected
- Distribution of files by origin (i.e. whether they've been associated with a component from a previous scan, the component catalog, the SCA database or local)
- Distribution of components by category (i.e. proprietary, Open Source, excluded, etc.)
- Distribution of component by obsolescence level, based on the detected version and the latest known version of each component
- Distribution of components by license compliance

- Distribution of components by vulnerability level (e.g. critical, high, medium, etc.)
- Distribution of components by license (e.g. MIT, Apache-2.0, etc.)
- Distribution of components by programming language (Java, Cobol, etc.)
- Distribution of components by topics (e.g. html5, devops, Angular, visualization, etc.)
- Distribution of components by file extensions of scanned files

#### Components

							Showing	I to 16 of 16 < 1	> 100 / pa
Open Source	16	Name	Versions	Latest version 🗘	Obsolescence	Licenses	Files 🗘 Path		¢   🗖
Proprietary	1	Piero_93/progetto-pnb-ambo-raspi			Unknown		1 /Hyg	ieia-master/UI-tests/	actions
Excluded	0	gridstack	0.2.6	4.2.6	High	MIT	1 /Hyg	eia-master//etc/	actions
Sandbox	0	tinymce/tinymce	2.0.7	5.8.1	High CVE-2020-17480		1 /Hyg	eia-master//dashboar	
Undefined	0	CapitalOneCanada/capitalonecanada.github.io			Unknown		2 /Hyg	ela-master//src/	Show Files
		codeheroics/nope.			Unknown		1 /Hyg	eia-master//fonts/	Edit Component Change Category
		vburlay/rmarkdouwn	v0.6	v2.1	High		1 /Hyg	ela-master//fonts/	Add to Catalog
		roccojanse/efocus-boilerplate			Unknown		1 /Hyg	ela-master//fonts/	
		dcode-study-ethereum/truffle-react-bootstrap-box			Unknown		1 /Hyg	eia-master//fonts/	actions
		neocities/neocities	2.0.0	3.0.0	Medium	BSD-2-Clause	4 /Hyg	eia-master//fonts/	actions
		jdamick/dropwizard-metrics-cloudwatch	0.1.3	0.1.6	Outdated	Apache-2.0	1 /Hyg	eia-master/	actions
		VirtualEngine/AppvProvider	v0.6.0.4	v0.6.2.8	Outdated	Apache-2.0	1 /Hyg	eia-master/	actions
		angular-ads	1.0.0	1.5.0	Outdated	MIT	1 /Hyg	eia-master//src/	actions
		xiyouMc/ncmbot		v0.1.6	Unknown		1 /Hyg	ieia-master/	actions
		brettbourquin/maven-wrapper	maven-wrapper-0.1.3	maven-wrapper-0.4.0	High	Apache-2.0	3 /Hyg	eia-master/	actions
		Sing-Li/bbug	nodearm	nodearm	Outdated		1 /Hyg	ieia-master//images/	actions
		Hygiela/Hygiela	v3.1.0	v3.1.0	Up to date	Apache-2.0	471 /Hyg	iela-master/	actions

From this Components view, you can see the list of components that have been detected in a SBOM along with their associated information. Note that columns of this table can also be configured (hide/show).

- Name: name of the component
- Versions: detected version(s) of the component

- Latest Version: latest known version of the detected component
- Obsolescence: level of obsolescence of a given component based on the gap between the detected version and the latest known version of this component
- Vulnerabilities: list of known vulnerabilities for a given component version
- Licenses: license(s) of the component with a color indication of its compliance with the policy used for the current SBOM
- Path: path of the folder where the component has been detected
- SCA Id: technical identifier of the component as it appears in the CAST Highlight SCA database

From this view, the user can launch some actions for each component:

- Show Files: this will show the files that have been mapped to this component based on SHA256 fingerprints.
- Edit Component: this will open a modal where the user can edit information for a component (e.g. add/change a license, add a vulnerability, leave a comment, etc.) – Refer to the Component Edit section
- Change Category: this will change the category of a component based on user input. By default, known third-party components are categorized as being Open Source, unknown files fall into the "Uncategorized" category. However, users can change the category of a component such as Proprietary, Excluded, Sandbox.
- Add to Catalog: this will add the selected component to the catalog so that this component can be shared and retrieved across other SBOMs. Refer to the Catalog section.

#### File Map

							licy: GPL v3 compliance	Ехро
E Hygieia-master	+ Hygiela-master							
<ul> <li>Hygieia-master</li> </ul>	+ .github	+ certs	+ travis-utilities	Hygleia2.md	Ticket_26665_sourcet checkstyle.xml	circle.yml	docker-compose.ove	docker-c
● .github								
.mvn ⊕								
+ UI								
<ul> <li>UI-protractor-tests</li> </ul>								
<ul> <li>UI-tests</li> </ul>	+ .mvn	+ db	gitignore	LICENSE				
certs								
db								
<ul> <li>hiresults</li> </ul>					features.md	mvnw.cmd	package-lock.json	pmd.xml
<ul> <li>HLTemporary</li> </ul>								
HLAutomation.log	+ UI	+ hiresults	.travis.yml	MAINTAINERS				
🖃 media	- 01	- 111050115	.aravis.yna	MAIN TAINERS				
⊕ images								
README.md					hygiela.json			
<ul> <li>test-servers</li> </ul>								
<ul> <li>travis-utilities</li> </ul>								
🗅 .gitignore	+ UI-protractor-tests	+ media	CHANGELOG.md	README.md		pom.xml	rev-version.	sh wrag
🗅 .travis.yml					- mongoar e ja	1		
CHANGELOG.md								
Dockerfile								
Hygleia2.md								
LICENSE	+ UI-tests	+ test-servers	Dockerfile	Setup.md		release.md		
MAINTAINERS					mvnw			
README.md								
Setup.md								
Ticket_26665_sourceCodeWithInfraction	ions.							

This view allows users to navigate through the folder structure of the SBOM to visualize scanned files with their corresponding component information and license compliance.

You can edit file-level information and add a comment by selecting a file and clicking on the "Edit" button.

	Edit mongosrc.js			Х		
• .mvn	Details Info					
	Extension: j	S				
	Version:	v3.0.3			nd	
• UI	Licenses :	Apache-2.0 × gp		Q		
		GPL-1.0			on	
	Comments :	GPL-2.0			20	
		GPL-2.0-with-classpath-exception				
• UI-protractor-tests		GPL-3.0				
				11		
				ОК		
UI-tests	+ test-servers	Dockerfile	Setup.md			

### SBOM Export

Components	by Cate	egory	Components by Obsolesce	nce	
Proprietary	0				Outdated - 40 High - 13 Medium - 65
Open Source		Configure BOM Export	X		Low - 71 Up to date - 100
Sandbox	0				Unknown - 2
Excluded	0	Export BOM Components			
Undefined	1	Export BOM Files			
		✓ Export BOM KPIs			
			ОК		
Top 10 Com	ponents		UK	es	28
					java - 284
Apache-2.0 EPL-2.0		165 33			java - 204 javascript - 5
path-exception BSD-Family	14	30			

You can export SBOM information from any view of the SBOM/Project section. To do so, click on the "Export" button on the left of the header menu and select the content to be exported:

- Component information
- File information
- KPI information

•	Home Inse	rt Page Layout Formulas Data Review View	Help				남 Share 🖓 🖓	Comme
ult		→ III III III III V Ruler	🗹 Formula Bar		Split 🗠 View Side by Side			
	👁 Ecit 🔍 Nev		✓ Headings Zoom 100% Zo		e Freeze Hide ID Synchronous Scrolling	Switch Macros		
.eep ۹	eg Eat seg Nev	Preview Layout Views	Y Headings Se	lection Window All	Panes - 🛄 Unhide 📴 Reset Window Positio	Windows 👻 👻		
	Sheet View	Workbook Views	Show Zoom		Window	Macros		
	* : >	< √ f <sub>×</sub> OUTDATED						
D	E	F	G		н	L	к	
CA	central	Apache-2	.0	2.12.5	2.13.0	LOW	/WEB-INF/lib/	htt
CA	central			2.6.1	3.0.1	MEDIUM	/WEB-INF/lib/	htt
CA	central	Apache-2	.0	2.12.5	2.13.0	LOW	/WEB-INF/lib/	htt
CA	central	Apache-2	.0	1.9.13	1.9.13	OUTDATED	/WEB-INF/lib/	htt
A	central	CVE-2013-5979   CVE-2013-5960 BSD-Fami	ly   CC-BY-SA-3.0	2.0.1	2.2.3.1	MEDIUM	/WEB-INF/lib/	htt
A	central	LGPL-2.0		5.1.2.Final	5.1.2.Final	UPTODATE	/WEB-INF/lib/	htt
A	central	EPL-2.0		3.18.0	3.27.0	MEDIUM	/WEB-INF/lib/	htt
A	central	BSD-Fami	ly	1.03	1.06	MEDIUM	/WEB-INF/lib/	ht
A	central	Apache-2	.0	2.5.0	2.5.0	UPTODATE	/WEB-INF/lib/	ht
A	central	MIT		3.12.0	3.18.1	MEDIUM	/WEB-INF/lib/	htt
A	central	BSD-Fami	ly	7.1	9.2	HIGH	/WEB-INF/lib/	htt
A	central	Apache-2	.0	2.5.0	2.5.0	UPTODATE	/WEB-INF/lib/	htt
A	npmjs	CC-BY-4.0	MIT   OFL-1.1	5.15.4	6.0.0-beta2	MEDIUM	/js/node modules/@fortawesome/fontawesome-free/	htt
A	central	Apache-2	.0	6.2.4	6.2.6	LOW	/WEB-INF/lib/	htt
A	central	Apache-2	.0   SAX-PD   W3C	1.4.01	1.4.01	OUTDATED	/WEB-INF/lib/	
A	central	BSD-3-Cla	use	2.3.5	2.3.5	UPTODATE	/WEB-INF/lib/	ht
A	central	Apache-2	.0	1.5.24	1.6.3	LOW	/WEB-INF/lib/	htt
A	central	CVE-2019-11269   CVE-2019-3778   CVE-2018-1 Apache-2	.0	2.1.0.RELEASE	2.5.1.RELEASE	MEDIUM	/WEB-INF/lib/	ht
A	central	Apache-2	.0	5.3.10	5.3.12	LOW	/WEB-INF/lib/	ht
A	central	Apache-2	.0	5.5.4	5.5.5	UPTODATE	/WEB-INF/lib/	ht
A	central	Apache-2	.0	5.3.10	5.3.12	LOW	/WEB-INF/lib/	ht
A	central	Apache-2	.0	5.3.10	5.3.12	LOW	/WEB-INF/lib/	ht
A	central	Apache-2	.0	3.14	4.1.2	MEDIUM	/WEB-INF/lib/	ht
A	central	BSD-2-Cla	use	42.2.20	42.3.0	LOW	/WEB-INF/lib/	ht
A	central	CC0-1.0		1.0.3	1.0.3	UPTODATE	/WEB-INF/lib/	ht
A	central	Apache-2	.0	1.5.1	1.5.4	OUTDATED	/WEB-INF/lib/	ht
A	central	NOASSER	TION Apache-2.0	1.2	1.2	UPTODATE	/WEB-INF/lib/	ht
A	central	Apache-2		3.14.15	3.15.3	LOW	/WEB-INF/lib/	ht
A	central	Apache-2		3.14.15	3.15.3	LOW	/WEB-INF/lib/	ht
A	central		TION   Apache-2.0	2.2.14	2.2.14	UPTODATE	/WEB-INF/lib/	ht
A	central	Apache-2		3.14.15	3.15.3	LOW	/WEB-INF/lib/	ht
A.	central		GPL-2.0-with-classpath-exception		3.0.3	MEDIUM	/WEB-INF/lib/	ht
Ą	central		MPL-1.1   Apache-2.0	3.27.0-GA	3.28.0-GA	LOW	/WEB-INF/lib/	ht
A.	central		GPL-2.0-with-classpath-except		2.3.1	UPTODATE	/WEB-INF/lib/	ht
A	central			1.0	1.0.1	OUTDATED	/WEB-INF/lib/	
A	central	GPL-2.0-v	vith-classpath-exception   EPL-2		1.6.7	UPTODATE	/WEB-INF/lib/	ht
					21017			

The SBOM export is currently available in Excel format.

### Catalog

In the SCAR SBOM Manager, the catalog is a central repository which allows the sharing of components across SBOMs. Using the catalog will help users capitalize on the qualification effort spent for each SBOM, including for managing proprietary components, component exclusions, component approval processes, etc.

C/ST
------

						Showing	1 to 12 of 12 < 1 >	25 / pag
Open Source	12	Name ¢	Versions	Latest version 💠	Obsolescence	Licenses	SCA Id	
Proprietary	2	com.thoughtworks.xstream:xstream-jmh	1.4.18	1.4.18	Up to date	BSD-3-Clause	com.thoughtworks.xstream:xstr	actions
Excluded	1	org.springframework:spring-context	5.3.10	5.3.12	Low	Apache-2.0	org.springframework:spring-cor	actions
Sandbox	0	org.springframework.boot:spring-boot-autoconfigure	2.5.5	2.5.6	Up to date	Apache-2.0	org.springframework.boot:sprin	actions
Undefined	0	org.springframework.security.extensions:spring-security-saml2-core	1.0.3.RELEASE	1.0.10.RELEASE	Low	Apache-2.0	org.springframework.security.ex	actions
		org.springframework.integration:spring-integration-jmx	5.5.4	5.5.5	Up to date	Apache-2.0	org.springframework.integration	actions
		org.springframework.integration:spring-integration-http	5.5.4	5.5.5	Up to date	Apache-2.0	org.springframework.integration	actions
		org.apache.velocity:velocity	1.7	1.7	Outdated	Apache-2.0	org.apache.velocity:velocity	actions
		com.googlecode.libphonenumber:libphonenumber	8.11.1	8.12.35	Low	Apache-2.0	com.googlecode.libphonenumb	actions
		net.java.dev.jna:platform	3.4.0	3.5.2	Outdated	LGPL-2.1	net.java.dev.jna:platform	actions
		com.sun.mail:pop3	1.6.7	1.6.7	Up to date	EPL-2.0 GPL-2.0-with-classpath-exception	com.sun.mail:pop3	actions
		neocities/neocities	2.0.0	3.0.0	Medium	BSD-2-Clause	neocities/neocities	actions
		gridstack	0.2.6	4.2.6	High	MIT	gridstack.npm	actions

#### **Component Categories**

This view lists all components which have been previously added to the catalog,

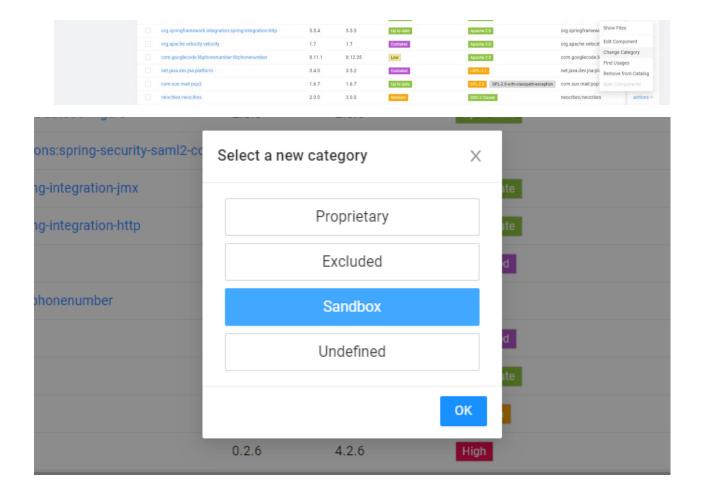
distributed by component category:

- Open Source
- Proprietary
- Excluded
- Sandbox
- Undefined

Clicking on a category on the top left list will refresh the component table.

To change the category of a component, click on "actions" for a given component, then click on "Change Category". A modal will open to select the new category to be applied to the component.

### CAST SBOM Manager



You can also change the category of multiple components by checking component boxes and clicking on "Actions" on top left of the screen.

企									+ New BOM	Ø 🌣	
Ð	Catalog License policy: My Policy Export										
• <b>G</b>	Actions V								Showing 1 to 6 of 6 < 1 >	50 / page $ \lor $	
E	Clear selection	0		Name 👙	Versions	Latest version $\ \ \diamondsuit$	Obsolescence 🗘 Vulnerabilities	Licenses	SCA Id 💠	•	
Ö		1	<b>V</b>	commons-httpclient:commons-httpclient	3.1	3.1	Outdated		commons-httpclient:commons-httpclient	actions 🗸 🧍	
_ ¢	Remove from Catalog	0	<b>~</b>	com.jayway.jsonpath:json-path-assert	2.4.0	2.4.0	Up to date	TOTO Apache-2.0	com.jayway.jsonpath:json-path-assert	actions V	
105 1	Change Category	0	<b>~</b>	com.google.protobuf:protobuf-java	2.4.1	3.13.0	Medium	BSD-3-Clause-Clear	com.google.protobuf:protobuf-java	actions 🗸	
	Merge Components	0	<b>V</b>	org.springframework:spring-context-support	4.3.19.RELEASE	5.2.8.RELEASE	Medium	Apache-2.0	org.springframework:spring-context-support	actions ~	
	Split Components	_		org.springframework:spring-web	4.3.19.RELEASE	5.2.8.RELEASE	Medium	Apache-2.0	org.springframework:spring-web	actions ~	
				org.opensaml:xmltooling	1.4.1	1.4.4	Outdated	Apache-2.0	org.opensaml:xmltooling	actions V	

All component changes (description, licenses, vulnerabilities, versions, etc.) made from the Catalog view will be saved for further SBOMs when the catalog option is active during the SBOM creation.

#### Propagate component changes in SBOMs

You also have the option to propagate component information changes to existing SBOMs that have this component. To do so, check the box below prior to clicking to the "Save" button.

Vulnerabilities :	CVE-2019-8331 x CVE-2020-17480 x CVE-2021-23926 x CVE-2021-28168 x	Comments :	
Licenses:	Apache-2.0 ×		
	Apply license changes to files		
Cancel			Apply changes to linked born component Save

#### Find component usage across SBOMs

You can easily retrieve all SBOMs that have a specific component from the catalog. To do so, click on actions > Find Usages for a given component.

com.thoughtworks.xstream:xstream-jmh	1.4.18	1.4.18	Up to date	BSD-3-Clause	com.thoughtworks	xstream:xstr actions v
org.springframework:spring-context	5.3.10	5.3.12	Low	Apache-2.0	org.springframewo	Show Files
org.springframework.boot:spring-boot-autoconfigure	2.5.5	2.5.6	Up to date	Apache-2.0	org.springframewo	Edit Component
org.springframework.security.extensions:spring-security-saml2-core	1.0.3.RELEASE	1.0.10.RELEASE	Low	Apache-2.0	org.springframewo	Change Category
org.springframework.integration:spring-integration-jmx	5.5.4	5.5.5	Up to date	Apache-2.0	org.springframewo	Remove from Catalog
org.springframework.integration:spring-integration-http	5.5.4	5.5.5	Up to date	Apache-2.0	org.springframewo	Split Components

Click on a SBOM to directly access it.



Excluded Sandbox Undefined	0	org.springframework.spring-context	Usages of Component net.java.dev.jna:platform	×	Apaster2.0	org.springframework:spring-cor	
		org.springframework.boot.spring-boot-auto			The second secon	org springhous work spring-cor	actions ~
Undefined			Product : Portal		Apache-2.0	org.springframework.boot.sprin	actions
		org.springframework.security.extensions.sp	Project : SpringBoot	¢	Apathe 2.0	org.springframework.security.e:	actions
		org.springframework.integration.spring-inte	Version: 2.5.5		Apathe2.0	org.springframework.integration	actions
		org springframework integration spring-inte			Abache 2.0	org.springframework.integration	actions
		org.apache.velocity:velocity			Apothe 2.0	org.apache.velocity.velocity	actions
		com.googlecode.libphonenumber.libphoner			Apache 2.0	com.googlecode.libphonenumb	actions
		net.java.dev.jna.platform			107-21	net.java.dev.jna:platform	actions
		Com.sun.mail.pop3			6PL-2.0-with-classpath-exception	com.sun.mail.pop3	actions
		neocities/neocities			85D-2-Clause	neocities/neocities	actions
		gridstack			MIT	gridstack.npm	actions

### Licenses

The SBOM Manager enables users to visualize, edit and even create licenses along with updating/defining license properties for each.

The main view lists supported licenses that are automatically detected in SBOMs:

- SPDX identifier
- License title
- Properties: permissions, constraints, and other properties of a license, summarized with icons
- Actions: edit or delete the license

2	Licenses > Management	Policies	+ New I	юм 🔗 🌣
<u></u>	Create a new License			
			Showing 1 to 25 of 129 < 1 2 3 4 5 6	> 25 / page 🗸
G s	SPDX 💠	Title 💠	Properties	
2 0	DBSD	BSD Zero Clause License	W / A 5 17 2 0 0 0	actions V
A	AFL-2.0	Academic Free License v2.0	W Z S 2 🗃 🛛 🔲 🔘	actions V
3	AFL-3.0	Academic Free License v3.0	H / 5 7 <b>8 10 0 10 0 1</b> 0 10 0	Edit License
	AGPL-1.0	Affero General Public License v1.0		Delete License
٨	AGPL-3.0	Affero General Public License v1.0	M / 5 2 <b>8 1 3 8 8 1 4 6 9</b> 8	actions V
٨	Aladdin	Aladdin Free Public License	H / M S V R 8 0 b	actions V
٨	AML	Apple MIT License	M / S / M M 0 B 0	actions $\vee$
A	Apache-1.0	Apache License 1.0	W / 5 7 <b>0 10 6 8 0 10</b>	actions $\vee$
A	Apache-1.1	Apache License 1.1	W / 5 7 <b># 14 8 8 1 0</b> 1 10	actions $\vee$
A	Apache-2.0	Apache License 2.0	W / A 5 7 8 🕅 M 3 8 🖩 🖬 🕸 🗰 🖗 🕼	actions $\vee$
A	Apache-Family			actions $\vee$
A	APL-1.0	Adaptive Public License 1.0	W / S R 💋 M 8 🕊 B 🖩 🕫 G	actions V
4	APSL-1.1	Apple Public Source License 1.1		actions V
4	APSL-1.2	Apple Public Source License 1.2		actions $\vee$
A	APSL-2.0	Apple Public Source License 2.0	W / 5 12 8 <b>6 19 6 8 6 9 10</b> 10	actions Y
A	Artistic-1.0	Artistic License 1.0	z 5 7 🕅 🖬 8 8 19 10 10	actions $\gamma$
A	Artistic-2.0	Artistic License 2.0	W Z S Z 🗃 🖬 🖪 🛛 🖗 🗰 🚳	actions $\vee$
B	Beerware	Beerware License	₩ 2 5 12 8 0	actions $\vee$
B	3SD-1-Clause	BSD 1-Clause License	🖉 S 🖓 🕑 🛢 🗢	actions $\vee$

To edit a license, click on its SPDX identifier or select "Edit License" from the "actions" menu.

#### **Create/Edit a license**

From the "Info" tab, you can modify:

- The license title
- The license description
- The license category (Public Domain Like, Permissive, Weak Copyleft, Strong Copyleft, Restrictive...)



Licenses > Manager		_				
Create a new License		Edit License AGP	L-1.0 - Affero General Public License v1.0	×		
		Info Proper	ties Details		Showing 1 to 25 of 138 < 1 2 3 4 5 6 >	25 / pa
SPDX	Title	► Spdx :				
OBSD	BSD Zero Clause License	• Title :	Affero General Public License v1.0			actions
AFL-2.0	Academic Free License v2.0					actions
AFL-3.0	Academic Free License v3.0	Description :				actions
AGPL-1.0	Affero General Public License v1.0			li.		actions
AGPL-3.0	Affero General Public License v1.0	Category:	Strong copyleft	~		actions
Aladdin	Aladdin Free Public License	gory -	Unknown			actions
AML	Apple MIT License		Public Domain like			actions
Apache-1.0	Apache License 1.0		Permissive			actions
Apache-1.1	Apache License 1.1		Weak copyleft			actions
Apache-2.0	Apache License 2.0		Strong copyleft Restrictive			actions
Apache-Family			Restrictive			actions
APL-1.0	Adaptive Public License 1.0					actions
APSL-1.1	Apple Public Source License 1.1					actions
APSL-1.2	Apple Public Source License 1.2					actions
APSL-2.0	Apple Public Source License 2.0					actions
Artistic-1.0	Artistic License 1.0					actions
Artistic-2.0	Artistic License 2.0					actions
Artistic-Family						actions
Beerware	Beerware License					actions
BSD-1-Clause	BSD 1-Clause License			_		actions
BSD-2-Clause	BSD 2-Clause "Simplified" License	Cancel		ок		actions

From the "Properties" tab, you can modify the different properties of the edited license. Check or uncheck the properties you want to edit and click "OK" to save your changes for a given license.

Create a new License		Edit License 0BSD - BSD Zero Clause License	×	
		Info Properties Details	Sho	owing 1 to 25 of 138 < 1 2 3 4 5 6 > 25 / 1
SPDX	≑ Title	CAN - 6/6	>	
OBSD	BSD Zero Clause License	CANNOT - 1/5	>	action
AFL-2.0	Academic Free License v2.0	MUST - 0/7	>	action
AFL-3.0	Academic Free License v3.0	FOR - 1/2	>	action
AGPL-1.0	Affero General Public License v1.0	SUPPORT - 1/4	×	action
AGPL-3.0	Affero General Public License v1.0			action
Aladdin	Aladdin Free Public License			action
AML	Apple MIT License			action
Apache-1.0	Apache License 1.0			action
Apache-1.1	Apache License 1.1			action
Apache-2.0	Apache License 2.0		0	] action
Apache-Family				action
APL-1.0	Adaptive Public License 1.0			action
APSL-1.1	Apple Public Source License 1.1			action
APSL-1.2	Apple Public Source License 1.2			action
APSL-2.0	Apple Public Source License 2.0			action
Artistic-1.0	Artistic License 1.0			action
Artistic-2.0	Artistic License 2.0			action
Artistic-Family				action
Beerware	Beerware License			action
BSD-1-Clause	BSD 1-Clause License			action
BSD-2-Clause	BSD 2-Clause "Simplified" License	Cancel	ОК	action

C/ST

From the "Details" tab, you can modify the license url and eventually paste the original license text.

ର	Licenses > Management	Policies	_						- N	W BOM
	Create a new License		Edit License	e OBSD - E	ISD Zero C	ause License		×		
			Info	Properties	Details				Showing 1 to 25 of 138 < 1 2 3 4 5 6	> 25/page V
00	SPDX	Title		URL:						
2	OBSD	BSD Zero Clause License		Text:						actions 🗸 🌰
ġ	AFL-2.0	Academic Free License v2.0		Text. 1						actions ~
ŵ	AFL-3.0	Academic Free License v3.0								actions ~
~	AGPL-1.0	Affero General Public License v1.0								actions ~
	AGPL-3.0	Affero General Public License v1.0								actions ~
	Aladdin	Aladdin Free Public License								actions ~
	AML	Apple MIT License						11		actions ~
	Apache-1.0	Apache License 1.0								actions ~
	Apache-1.1	Apache License 1.1								actions ~
	Apache-2.0	Apache License 2.0							0	actions ~
	Apache-Family									actions ~
	APL-1.0	Adaptive Public License 1.0								actions ~
	APSL-1.1	Apple Public Source License 1.1								actions ~
	APSL-1.2	Apple Public Source License 1.2								actions ~
	APSL-2.0	Apple Public Source License 2.0								actions ~
	Artistic-1.0	Artistic License 1.0								actions ~
	Artistic-2.0	Artistic License 2.0								actions ~
	Artistic-Family									actions ~
	Beerware	Beerware License								actions ~
	BSD-1-Clause	BSD 1-Clause License						_		actions ~
	BSD-2-Clause	BSD 2-Clause "Simplified" License	Cancel					ок		actions 🗸

#### Create/Edit a license policy

You can define or edit license policies. A license policy is a set of rules that will define the level of risk or acceptance for a given list of licenses.

From the main License view, click on "Policies" in the breadcrumb on top of the page. You can switch between policies and view the corresponding compliance table for each license.

License compliance has four different properties:

- Compliant
- Partially compliant, under conditions
- Not compliant
- Undefined compliance



GPL v3 compliance V ASL 3rd party compliance	Create new Policy Edit Policy Make Default Delete Policy	
GPL v3 compliance		Showing 1 to 10 of 74 < 1 2 3 4 5 ··· 8 >
My App License Policy		Compliance
My Policy	BSD Zero Clause License	Ø © ⊗ ?
AFL-2.0	Academic Free License v2.0	S (2) (2) (2)
AFL-3.0	Academic Free License v3.0	S (S) (S)
AGPL-1.0	Affero General Public License v1.0	) 😒 🔾
AGPL-3.0	Affero General Public License v1.0	⊘ ⊗ ③
Aladdin	Aladdin Free Public License	) 🛇 O
AML	Apple MIT License	⊙ ⊗ ⊙
Apache-1.0	Apache License 1.0	) 🛇 O
Apache-1.1	Apache License 1.1	) 🛇 O
Apache-2.0	Apache License 2.0	⊙ ⊗ ⊙

To edit compliance properties of a license in a license policy, simply check/uncheck compliance property icons.

To remove a license from a license policy, click on the trash icon.

To add a license to a license policy, click on the "Add License" button on top right of the screen.



C C C C C C C C C C C C C C C C C C C	Create new Policy	Edit Policy Make Default Delete Policy Add License Compliance	Showing 1 to 10 of 74 < 1 2	Compliance ⊘ ⓒ ⊗ ?	Add License
SPDX           08SD           1           04SD           05           1           05           1 <t< th=""><th>BSD Zero Academic Academic</th><th></th><th></th><th>Compliance ⊘ ⓒ ⊗ ?</th><th>¢      </th></t<>	BSD Zero Academic Academic			Compliance ⊘ ⓒ ⊗ ?	¢
SP0X       0BSD       AFL-2.0       AFL-3.0       AGPL-3.0       AGPL-3.0       Aladdin       AML	BSD Zero Academic Academic		×	⊙ ⊗ ⊙	
AFL-2.0 AFL-3.0 AGPL-1.0 AGPL-3.0 Aladdin AML	Academic Academic		×		n 1
AFL-3.0 AGPL-1.0 AGPL-3.0 Aladdin AML	Academic	excention			
AGPL-1.0 AGPL-3.0 Aladdin AML		exception		⊙ ⊙ ⊗ ?	Û
AGPL-1.0 AGPL-3.0 Aladdin AML	Afforo Co	cxocption		○ ○ ○ ○	Ū
Aladdin AML	Affelo Ge	GPL-Family		() () () () () () () () () () () () () (	Ū
AML	Affero Ge	GRI Greg's License			Û
	Aladdin F	HPND Historical Permission Notice and Disclai	mer	0 0 🛇 🔿	Ū
Anacha 1.0	Apple MI	JSON JSON License	$\odot$	$\odot$ $\odot$ $\odot$	Ū
Apache-1.0	Apache L	LGPL-Family under condition		0 🖸 🛇	Ū
Apache-1.1	Apache L			0 0 🛇 🔿	Û
Apache-2.0	Apache L	Compliance Level : 🕢 🜔 🗙 🕐		$\odot$ $\odot$ $\odot$	Ū.
		Cancel	Save		

Select the license you want to add and define the compliance level, then click on the "Save" button.

You can make a specific license policy the default policy to apply when creating a SBOM, by clicking on the "Make Default" button on top of the screen.

Finally, you can completely remove a license policy by clicking on the "Delete Policy" button on top of the screen.

### Vulnerabilities

CAST Highlight's SBOM Manager automatically detects CVEs (Common Vulnerabilities & Exposures) in scanned third-party components, but also allows users to manually log vulnerabilities in Open Source or even internal components, such as security issues or bugs. This section details how it works.

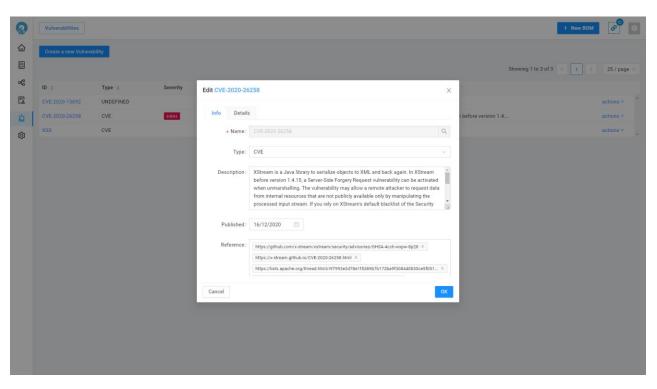
### **CAST SBOM Manager**

୍ଲ	Vulnerabilities					+ New BOM
습	Create a new Vuln	erability Delete	all unlinked Vulne	rabilities		
ΠŊ					Showing 1 to 25 of 30 < 1	2 > 25/pa
o[0	ID \$	Туре	C Severity	¢ CWE	Description	
2	Bug-10029	UNDEFINED				actions
ă	CVE-2012-5783	CVE	MEDIUM	CWE-295	Apache Commons HttpClient 3.x, as used in Amazon Flexible Payments Service (FPS) merchant Java SDK a	Edit Vulnerability
¢	CVE-2013-4002	CVE	HIGH		XMLscanner.java in Apache Xerces2 Java Parser before 2.12.0, as used in the Java Runtime Environment	Delete Vulnerability Find vulnerable BOMs
~	CVE-2013-5960	CVE	MEDIUM	CWE-310	The authenticated-encryption feature in the symmetric-encryption implementation in the OWASP Enterpr	actions
	CVE-2013-5979	UNDEFINED				actions
	CVE-2014-3603	CVE	MEDIUM	CWE-297	The (1) HttpResource and (2) FileBackedHttpResource implementations in Shibboleth Identity Provider	actions
	CVE-2014-3604	CVE	MEDIUM	CWE-310	Certificates.java in Not Yet Commons SSL before 0.3.15 does not properly verify that the server host	actions
	CVE-2015-7501	CVE	CRITICAL	CWE-502	Red Hat JBoss A-MQ 6.x; BPM Suite (BPMS) 6.x; BRMS 6.x and 5.x; Data Grid (JDG) 6.x; Data Virtualiza	actions
	CVE-2016-10735	UNDEFINED				actions
	CVE-2017-12626	CVE	HIGH	CWE-835	Apache POI in versions prior to release 3.17 are vulnerable to Denial of Service Attacks: 1) Infinit	actions
	CVE-2017-18349	CVE	CRITICAL	CWE-20	parseObject in Fastjson before 1.2.25, as used in FastjsonEngine in Pippo 1.11.0 and other products,	actions
	CVE-2017-5644	CVE	MEDIUM	CWE-776	Apache POI in versions prior to release 3.15 allows remote attackers to cause a denial of service (C	actions
	CVE-2018-14040	UNDEFINED				actions
	CVE-2018-14042	UNDEFINED				actions

The main Vulnerabilities view lists all vulnerabilities detected across the different SBOMs. This data table contains:

- The identifier of the vulnerability
- The type (CVE, undefined, etc.)
- The severity (based on CVSS scores): low, medium, high, critical
- The nature (CWE) of the vulnerability
- A short description of the vulnerability
- Possible actions associated with a vulnerability (edit, delete, find vulnerable SBOMs)





#### Edit a vulnerability

To edit a vulnerability, click on its identifier, severity level or "Edit Vulnerability" from the Actions menu. A modal opens where you can edit the different properties of a vulnerability:

- The type (CVE, Undefined)
- The description
- The publish date
- The references (url to external websites)

From the "Details" tab, you can also edit:

- The different CWEs associated with a vulnerability
- Indicate parameters of CVSS scores (versions 2 and 3) that are used to calculate the severity level of the vulnerability

Click on the "OK" button to save the modified vulnerability information.



Ø	Vulnerabilities					+ New BOM
企	Create a new Vulnera	bility				
		_				Showing 1 to 3 of 3 $<$ 1 $>$ 25 / page $\vee$
어음	ID ¢	Туре 🗘	Severity	CWE Description		
E.	CVE-2020-13692	UNDEFINED		BOM vulnerable to 'CVE-2020-13692'	×	actions ~
Ö	CVE-2020-26258	CVE	HIGH	[c	n XStream before version	n 1.4 actions Y
\$	XSS	CVE		Product: MyCRM Project: Core Version: 1.0.1-beta	¢	actions ∨ +
					Close	

#### Find vulnerable SBOMs

You can easily find vulnerable SBOMs which have a given vulnerability by clicking "Find Vulnerable SBOMs" from the Actions menu. The list of SBOMs will be displayed with a direct link to each.

ର	Vulnerabilities						+ New BOM	Ø 🔹
습	Create a new Vulnera	bility						
IJ							Showing 1 to 3 of 3 < 1 >	25 / page \vee
0(0	ID ¢	Туре 💠	Severity	Create a new Vul	nerahility	×		
F	CVE-2020-13692	UNDEFINED		oreate a new van		~		actions V
ä	CVE-2020-26258	CVE	HIGH	Info Detail:	3		before version 1.4	actions ~
ŵ	XSS	CVE		* Name:	VULN	Q		actions Y
Ū				Type :	UNDEFINED			
				Description:	New <u>yulnerability</u> .			
						h		
				Published:	06/07/2021			
				Reference:	+			
				Cancel		ОК		

#### Log a vulnerability

You can manually log a vulnerability that will be associated with a component in SBOMs. It is also possible to automatically populate vulnerability information by entering the vulnerability identifier, in case this is a CVE from the National Vulnerability Database (NVD). Type the identifier (e.g., CVE-2020-26258) and click on the magnifying glass icon. Click on the "OK" button to save this vulnerability.



ର	Vulnerabilities					+ New BOM	<i>8</i>
企	Create a new Vulneral	bility					
					Q Would you like to search for 'CVE-2020-		25 / name V
너물					26258' and auto fill the form ?		237 page V
2	ID ¢ CVE-2020-13692	Type 0	Severity	Create a new Vuln	Cancel		actions 🗸 📍
ti l		CVE	HIGH	Info Details	1.6		actions ~
\$		CVE		* Name:	CVE-2020-26258 Q		actions Y
~~				Type:	CVF		
				Description:	New <u>vulnerability</u> .		
				L			
				Published:	06/07/2021		
				Reference :	+		
				Cancel			
_							
0	Mulmarshilltion					J. New POM	
ଛ	Vulnerabilities					+ New BOM	8
奋	Vulnerabilities Create a new Vulnerab	bility				+ New BOM	0
6) 12	American	bility					25 / page v
(j)	Create a new Vulnerat	bility Type ©	Severity	Create a new Vuln	erability ×		25 / page ~
(j) 19 19 19	Create a new Vulnerat	Type t				Showing 1 to 3 of 3 < 1 >	actions Y
	Create a new Vulnerat	Type : UNDEFINED CVE	Severity	Info Details	16	Showing 1 to 3 of 3 < 1 >	actions ~
(j) 19 19 19	Create a new Vulnerat	Type t		Info Details Severity:	нан 🗸	Showing 1 to 3 of 3 < 1 >	actions Y
	Create a new Vulnerat	Type : UNDEFINED CVE		Info Details Severity:	16	Showing 1 to 3 of 3 < 1 >	actions ~
	Create a new Vulnerat	Type : UNDEFINED CVE		Info Details Severity:	нан 🗸	Showing 1 to 3 of 3 < 1 >	actions ~
	Create a new Vulnerat	Type : UNDEFINED CVE		Info Details Severity: CWE: CVSS V	нан 🗸	Showing 1 to 3 of 3 < 1 >	actions ~
	Create a new Vulnerat	Type : UNDEFINED CVE		Info Details Severity: CWE: CVSS V	HIGH         V           CWE918 X         +           AV:N/ACL/AuxN/C9/IN/AN	Showing 1 to 3 of 3 < 1 >	actions ~
	Create a new Vulnerat	Type : UNDEFINED CVE		Info Details Severity: CWE: CVSS V V2 Vector:	HIGH         V           CWE918 X         +           AV:N/ACL/AuxN/C9/IN/AN	Showing 1 to 3 of 3 < 1 >	actions ~
	Create a new Vulnerat	Type : UNDEFINED CVE		Info Details Severity: CWE: CVSS V V2 Vector: V2 Scores: E CVSS V	HIGH         V           CWE918 X         +           AV:N/ACL/AuxN/C9/IN/AN	Showing 1 to 3 of 3 < 1 >	actions ~
	Create a new Vulnerat	Type : UNDEFINED CVE		Info Details Severity: CWE: CVSS V V2 Vector: V2 Scores: E CVSS V V3 Vector:	HICH     Image: Comparison of the second secon	Showing 1 to 3 of 3 < 1 >	actions ~
	Create a new Vulnerat	Type : UNDEFINED CVE		Info Details Severity: CWE: CVSS V V2 Vector: V2 Scores: E CVSS V	HICH     Image: Comparison of the second secon	Showing 1 to 3 of 3 < 1 >	actions ~
	Create a new Vulnerat	Type : UNDEFINED CVE		Info Details Severity: CWE: CVSS V V2 Vector: V2 Scores: E CVSS V V3 Vector:	HICH     Image: Comparison of the second secon	Showing 1 to 3 of 3 < 1 >	actions ~
	Create a new Vulnerat	Type : UNDEFINED CVE		Info Details Severity: CWE: CVSS V V2 Vector: V2 Scores: E CVSS V V3 Vector: V3 Scores: E	HIGH     Image: Constraint of the second secon	Showing 1 to 3 of 3 < 1 >	actions ~
	Create a new Vulnerat	Type : UNDEFINED CVE		Info Details Severity: CWE: CVSS V V2 Vector: V2 Scores: E CVSS V V3 Vector: V3 Scores: E	HIGH     Image: Constraint of the second secon	Showing 1 to 3 of 3 < 1 >	actions ~
	Create a new Vulnerat	Type : UNDEFINED CVE		Info Details Severity: CWE: CVSS V V2 Vector: V2 Scores: E CVSS V V3 Vector: V3 Scores: E	HIGH     Image: Constraint of the second secon	Showing 1 to 3 of 3 < 1 >	actions ~

### Preferences & Configuration

You can set a series of options and preferences for the SBOM Manager.





୍ଭ	Configuration	> General	BOM/Catalog	Scanner	System							+ New BC	M	G	\$
습															
Ð	General confi	guration													
ъľо	* Usage :	🖉 Browser (rec	ommended)	$\sim$											
2	* Email:	Desktop													
ò	Save	@ Browser (rec	ommended)												
¢															
~															

From the General element of the breadcrumb, you can retrieve the e-mail address associated with your user account. You can also switch from the Desktop mode to the Browser mode (recommended for better experience).

### CAST SBOM Manager



Bill of	Materials preferences	
	Move split components to the 'Sandbox' category:	
	Move merged component to the 'Sandbox' category:	
Apply	component license changes to associated files by default:	
	Apply added file licenses to parent component by default:	
The l	e settings apply to editing components and files associated with a particular BOM. ast two settings respectively specify whether to enable by default the option to propagate license ges made to BOM components and files.	
Catalo	g preferences	
	Move split components to the 'Sandbox' category:	
	Move merged component to the 'Sandbox' category:	
	Apply changes to linked BOM components by default:	
Apply	component license changes to associated files by default:	
	Apply added file licenses to parent component by default:	
The l	e settings apply to editing components and files associated with the Catalog. ast two settings respectively specify whether to enable by default the option to propagate license ges made to Catalog components and files.	
Save		

From the SBOM/Catalog breadcrumb element, you can define some options when creating a SBOM (e.g., moving a split component to the 'Sandbox' category by default) or using the Component Catalog (e.g., applying changes to a component or license ... in SBOMs when this object is updated in the catalog).

Configuration > Gen	eral BOM/Catalog Scanner System	+ New B	м
Scanner preferences			
Root folder:	Eb Select a Folder	Select	
	This path is used as the root of the file-system when selecting the codebase to scan.		
Maven repository folder:	😕 Select a Folder	Select	
	This path is used to facilitate the retrieval of component informatio using the Maven scanner and must point to the folder where all the artifacts are stored (eg. <u>C:/Users/John/ m2/repository</u> ).		

C/ST

From the Scanner element of the breadcrumb, you can define preferences related to scans (e.g., define the default root folder for scans, Maven repository folder).

Configuration > Ger	heral BOM/Catalog Scanner System	+ New BOM	Ø	ŝ
Application				
Varaian	1.0.0-RC2.adeed7a			
User directory:				
	C:\Users\mmu\AppData\Local\Programs\SCAr			
System				
	Windows 10			
OS version : OS architecture :				
	andu4 172.27.192.1			
Java				
Java version :	1.8.0_321-b07			
	C:\Program Files\Java\jre18.0_321			
	Oracle Corporation			
JVM version:	25.321-b07 Oracle Corporation			
	Grace Corporation			
System Memory				
Total system memory:	17.053.348			
JVM max heap size:				
JVM current heap size:				
JVM used memory:				
JVM free memory:	912,354			
Browser				
Browser name:	Chrome			
Browser version:	102.0.5005.63			
	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36			
Screen resolution:				
Browser resolution:	1536 x 864			

Finally, the last element of the breadcrumb recaps the different details of your SBOM Manager installation and system supporting it (Operating System, Java version installed, system memory, browser, etc.).