Software bill of materials

SOFTWARE NAME	VERSION NUMBER	DATE

Document Version History

ISSUE NUMBER	DATE	AUTHOR

The purpose of this document is to enumerate the components used in the software listed in “Software name” in order to create an easy method to track where specific components are being used by the organization and any software vulnerabilities that might affect them. The table should include all internally developed components, open source and commercial external software, libraries, frameworks, firmware and any other software components used to build this software. This table shows the main component name and any subdependencies. This is a hierarchical relationship where the component in question is itself reliant on other software, which can also be reliant on further software components, which have been included in the table as sub-subdependencies. This can be further deconstructed, but for the purposes of usability, the table does not list any further layers of dependencies.

Software components

COMPONENT NAME	SUPPLIER	VERSION	UNIQUE IDENTIFIERS (E.G., LICENSE INFORMATION)	RELATIONSHIP	SUB DEPENDENCIES	SUB-SUBDEPENDENCIES	AUTHOR	HASH	KNOWN VULNERABILITIES (CVE NUMBER)	DATE ADDED
Spring Framework—Spring Core	VMware Tanzu	5.3.18	Apache 2.0	Primary	Caffeine, Jackson, Reactor, Kotlin, Commons Logging, Byte Buddy, ASM, Objenesis, Log4j	Guava, SLF4J	John	0x123	CVE-2022-22971 CVE-2022-22970 CVE-2022-22968	10.25.24
Caffeine	Ben Manes	3.2.0	Apache 2.0	Third-party library included in			Bob	0x234	N/A	01.18.25
Jackson	Tatu Saloranta	2.13.1	Apache 2.0	Included in	Jackson Databind, Jackson Core, Jackson Annotation		John	0x567	CVE-2023-35116	02.04.25

Glossary

Component name: A main component of the software, such as commercial or internally developed software, firmware or an open source library.

Supplier: What vendor created this component.

Version: The current version of the component in use in the software. Update this if the version is updated.

License information: The owner of the license and any other relevant information, such as expiry.

Relationship: Whether this is the main component or a subdependency of another component.

Subdependencies: Any software components that are used by the component in the “Component name” column.

Sub-subdependencies: Any software components that are used by the component in the “Subdependencies” column.

Author: Who added this component information to the SBOM.

Cryptographic hash: An identifier to help with mapping the component.

Known vulnerabilities (CVE Number): A list of software vulnerabilities known to affect the component or any subdependencies. This should be listed using the Common Vulnerabilities and Exposures (CVE) number and a link to further information.

Date: When this component was added to the SBOM.