What is an SBOM, and why do software teams need one?

1 November 2026 · 5 min read · blogs.iictp.org/what-is-an-sbom

A software bill of materials (SBOM) is a machine-readable list of the components inside a piece of software, including their names, versions and where they came from. It lets a team answer one urgent question quickly: does this vulnerability affect anything we run?

TL;DR The short version

- An SBOM is a machine-readable list of the components in a piece of software, with names, versions and suppliers.
- It lets you answer quickly whether a newly announced vulnerability affects anything you run; SPDX and CycloneDX are the common formats.
- It does not make software secure by itself; generate it in the build pipeline and store it with each release.

Read online, listen to it, or change the text size: https://blogs.iictp.org/what-is-an-sbom

What does an SBOM contain?

It lists the components used, including indirect (transitive) dependencies, with each component's name, version and supplier. It records how the components relate to each other, and who produced the SBOM and when.

Which formats are used?

The two common open formats are SPDX and CycloneDX. Both can be generated by build tools and read by scanners, so an SBOM can move between a supplier, a customer and a security tool without being retyped.

Why does it matter?

When a flaw is announced in a widely used library, teams without an inventory spend days searching. With an SBOM per service, the search is a query. It also supports licence checks and supplier questions.

What does an SBOM not do?

It does not make software secure, and it does not say whether a listed vulnerability can actually be exploited in your use. Pair it with scanning and with statements about whether a flaw affects the product, such as VEX.

Who needs to produce and read one?

Anyone who ships software should be able to produce one, and anyone who buys or runs software benefits from reading one. Regulators and large customers increasingly ask for them, so building the habit early costs less than adding it under pressure.

How do you start?

Generate the SBOM in the build pipeline, not by hand, and store it with the release it describes. Scan it against vulnerability data on every build, and decide who reads the results and how quickly they must act.

Related credential: Certified Technical Practitioner. Explore the exam facts and syllabus.

Sources and further reading

1. NTIA. The Minimum Elements For a Software Bill of Materials (SBOM). ntia.gov.
2. CISA. Software Bill of Materials (SBOM). cisa.gov/sbom.
3. SPDX. spdx.dev. CycloneDX. cyclonedx.org.

Published by IICTP, an independent technical credential body, on 1 November 2026. The current version of this post is at https://blogs.iictp.org/what-is-an-sbom. More guides: blogs.iictp.org.