VCRI
THE VALUE CHAIN RISK INSTITUTE

VCRI LEARN · SOFTWARE SUPPLY CHAIN

What is an SBOM?

A software bill of materials: the ingredient list for the software you build and buy.

Joshua Marpet and Cairn Viktor

VCRI
THE VALUE CHAIN RISK INSTITUTE

WHY YOU CARE

“Are we affected?”

CVE is Common Vulnerabilities and Exposures, the public ID for a known flaw.
CISA is the US Cybersecurity and Infrastructure Security Agency.

December 2021

A flaw called Log4Shell (CVE-2021-44228) is found in Log4j, a Java logging library.

CISA calls Log4j “very broadly used” in consumer and enterprise services, websites and applications.

The hard question

Not “how do we fix it?” but “where is it?”

Log4j usually arrives buried inside other software. You cannot patch what you cannot find.

Source: CISA, Apache Log4j Vulnerability Guidance

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

THE IDEA IN ONE LINE

> *A software bill of materials is "a formal record containing the details and supply chain relationships of various components used in building software." "It is analogous to a list of ingredients on food packaging."*

US Executive Order 14028, Section 10(j), May 12, 2021

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

WHAT IS INSIDE

The minimum fields, per component

FIELD	WHAT IT ANSWERS
Supplier	Who made this component?
Component name and version	What is it, exactly which release?
Other unique identifiers	A precise ID tools can match, such as a package URL
Dependency relationship	Which component pulls in which?
Author and timestamp	Who wrote this SBOM, and when?

Source: NTIA, The Minimum Elements for a Software Bill of Materials, July 12, 2021. A cryptographic hash is a recommended extra field.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

DEPENDENCY RELATIONSHIPS

Ingredients have ingredients

NTIA describes software as a hierarchical tree of components and subcomponents. The relationships are what let you trace a flaw upward.

Your app
The code your team wrote, plus everything it pulls in.

→

A web framework
A direct dependency: you chose it on purpose.

→

A logging library
A transitive dependency: the framework chose it for you.

→

Its own parts
And so on down. A software tree can be many levels deep.

valuechainrisk.org/learn · CC BY 4.0

LOOK AT ONE

A tiny CycloneDX SBOM

```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.6",
  "components": [{
    "type": "library",
    "supplier": { "name": "Apache Software Foundation" },
    "group": "org.apache.logging.log4j",
    "name": "log4j-core",
    "version": "2.14.1",
    "purl": "pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1",
    "hashes": [{ "alg": "SHA-256",
                 "content": "(64 hex characters)" }]
  }]
}
```

Plain JSON
Readable by people, parsed by tools.

Name plus version
2.14.1 is inside the range CISA lists as affected by Log4Shell.

purl
Package URL: one exact ID that scanners match.

Hash
The file's fingerprint. A placeholder here; a real SHA-256 is 64 hex characters.

valuechainrisk.org/learn · CC BY 4.0

TWO MAIN FORMATS

SPDX and CycloneDX

Both carry the minimum fields. NTIA named both, plus SWID tags, as formats that meet the minimum elements.

SPDX

Software Package Data Exchange. An open standard hosted by the Linux Foundation.

Published as international standard ISO/IEC 5962:2021. Strong roots in license compliance.

CycloneDX

Developed under the OWASP Foundation and standardized as ECMA-424.

Built with security use cases in mind, including VEX (more on that soon).

Pick the one your tools and customers already use. Good tools convert between them.

Sources: spdx.dev; cyclonedx.org; NTIA Minimum Elements report

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

WHY NOW

Governments started asking

WHEN	WHAT HAPPENED
May 12, 2021	US Executive Order 14028 called for giving a purchaser an SBOM for each product, directly or on a public website.
July 12, 2021	NTIA published the minimum elements for an SBOM, the fields on our earlier slide.
Dec 10, 2024	The EU Cyber Resilience Act (CRA) entered into force. Annex I requires an SBOM covering at least top-level dependencies.
Dec 11, 2027	The CRA's main obligations apply to products sold in the EU.

Sources: EO 14028 Sec. 4(e)(vii); NTIA report; European Commission CRA policy page; CRA Annex I Part II(1)

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

LIMITS

An SBOM is not a vulnerability report

A snapshot

An SBOM describes one build at one point in time.

Vulnerability data keeps changing. Software that looked clean can “become” vulnerable when a new bug is found.

Present is not exploitable

A vulnerable library may sit in code that never runs.

VEX, Vulnerability Exploitability eXchange, is a supplier’s statement of whether a product is actually affected.

Only as good as its maker

An SBOM lists what the generator could see.

Missing components look exactly like absent ones.

Sources: NTIA Minimum Elements report (Vulnerabilities and SBOM; Vulnerability and Exploitability in Dependencies); CISA SBOM page

valuechainrisk.org/learn · CC BY 4.0

WHAT TO DO MONDAY

Start with two asks

- Ask your key vendors: can you give us an SBOM for the product we run, in SPDX or CycloneDX?
- Ask them a follow-up: do you publish VEX statements when a big vulnerability hits?
- Generate one for your own app with a free tool: `syft ./my-project` or `cdxgen -o bom.json .`
- Read the output. Count the components you did not know you had.
- Save it with the release, so next time someone asks “are we affected?” you search a file.

Tools: Syft (github.com/anchore/syft), cdxgen (github.com/cdxgen/cdxgen)

valuechainrisk.org/learn · CC BY 4.0

VCRI

THE VALUE CHAIN
RISK INSTITUTE

Free to use, teach and share.

This deck is part of the VCRI Learn series. Use it in your class, your team meeting or your chapter, with credit to The Value Chain Risk Institute.

valuechainrisk.org/learn

valuechainrisk.org/learn · CC BY 4.0