

Software Barrel of Monkeys (SBOM)

DJ Schleen

Distinguished Security Architect - Paranoids @ Yahoo

 @djschleen



A young boy with dark hair is shown from the chest up, looking down at an open book he is holding. He has a wide-eyed, excited expression. He is wearing a dark blue long-sleeved shirt with a pattern of white stars and constellations. The scene is set in a dark room, with a warm, glowing light source, possibly a fireplace, visible in the background to the right. The overall atmosphere is cozy and magical.

openssl story

What's inside?
Where did it come from?
Are there any vulnerabilities?

WHERE IS IT?

A man with a beard and dark hair, wearing a dark jacket and pants, stands in the center of the frame. Behind him is a massive, bright orange and yellow explosion that fills most of the background. Debris is flying through the air. The sky is a clear, bright blue. The overall scene is dramatic and action-oriented.

SBOM

Nutrition Facts

Serving Size 3 oz. (85g)
Serving Per Container 2

Amount Per Serving		Calories from Fat 120	
Calories	200	% Daily Value*	
Total Fat	15g		20 %
Saturated Fat	5g		28 %
Trans Fat	3g		
Cholesterol	30mg		10 %
Sodium	650mg		28 %
Total Carbohydrate	30g		10 %
Dietary Fiber	0g		0 %
Sugars	5g		
Protein	5g		
Vitamin A	5%	•	Vitamin C 2%
Calcium	15%	•	Iron 5%

*Percent Daily Values are based on a 2,000 calorie diet.
Your Daily Values may be higher or lower depending on your calorie needs.

	Calories	2,000	2,500
Total Fat	Less than	65g	80g
Sat Fat	Less than	20g	25g
	Less than	300mg	300mg
	Less than	2,400mg	2,400mg
	Less than	300mg	375mg
	Less than	20g	20g

BC





Jeep

DEALER TO WHOM DELIVERED
 LONGVIEW AMC AND JEEP, INC.
 1035 WANDERCOCK WAY
 LONGVIEW, PA
 MAKE OF VEHICLE: Jeep PRODUCTION FROM NO. A J 105342
 VIN: J3A17W078148 FINAL ASSEMBLY POINT: TOLEDO, OHIO MODEL: SE 4 45 276
 Manufacturer's Suggested Retail Price

SABLE BROWN, METALLIC		\$ 7,171.00
BEIGE BUCKET SEATS, M/CTR ARM REST		STD.
10X15 4X4 WHITE LTR TRACKER A/T		48.00
AXLE RATIO, 3.54/1		STD.
360 CID V-6 ENGINE, 2 BARREL		273.00
CONVENIENCE GROUP		STD.
HYDRA-PATIC 4 QUADRA-TRAC, LDR RAG		83.00
AIR CONDITIONING		449.00
POWER STEERING		49.00
TINTED WINDOW, TAILGATE		225.00
FUEL TANK SKID PLATE		73.00
ROOF RACK		51.00
GOLDEN EAGLE PROTRUD		69.00
TILT STEERING WHEEL		109.00
CRUISE CONTROL		75.00
AM/FM/CD STEREO RADIO		105.00
EXTRA-DUTY SUSPENSION PACKAGE		36.74.00
HEAVY-DUTY BATTERY, 70 AMP		121.00
REAR WINDOW DEFROSTER		38.00
PROTECTIVE FLOOR MATS		99.00
LEATHER-WRAPPED SPORT STRG WHEEL		19.00
DUAL MIRRORS-LOW PROFILE TYPE		21.00
CARPETED CARGO FLOOR & INSULATION		38.00
TRAILER TOWING PACKAGE "B"		74.00
STABILIZER BAR, FRONT		132.00
LIGHT GROUP		31.00
SOUND LEVEL CERTIFICATION PACKAGE		69.00
** ACCESSORY TOTAL **		16.00
		\$ 10,169.00

TRANSPORTATION CHARGES
 TOTAL AMOUNT DEC 18 1978 \$ 11,855.00

This label is affixed pursuant to Federal Automotive Information Disclosure Act. Dealer's price includes local taxes, dealer delivery and handling, and dealer installation. Dealer's price also includes optional accessories, license, title and license fees, and any other available accessories. Dealer's price does not include any other accessories. Dealer's price does not include any other accessories.
 Jeep Corporation
 Subsidiary of American Motors Corporation

- Jeep CJ
- Jeep Cherokee
- Jeep Wagoneer
- Jeep Truck

THE TOUGHEST
 4-LETTER WORD ON WHEELS.
Jeep

STANDARD FEATURES

- Electronic Ignition
- Parking Brake
- 4-Wheel Drive
- Rugged Leaf Spring Suspension
- Lime Changer Turn Signals*
- 4-Way Hazard Warning
- Automatic Back-Up Lights
- Electric Windows & Wipers
- Klaxon/Engine Chime
- Truck Rear-View Mirror
- Left-Hand Rear-View Mirror
- Side-Of-Car Safety Mirror Lights
- High-Strength Safety Glass
- Heated/Insulated Steering Wheel
- Power Disc Brakes, Front*
- Dual Master Brake Cylinder
- Corrosion-Resistant Brake Lines
- Front-Operated Parking Brake Pedals
- Suspended Clutch & Brake Pedals
- 3-Point Shoulder Lap Seat Belt*
- Tamper-Resistant Odometer
- Permanent-Type Anti-Freeze
- Tinted Sun Visors
- Dual Primary Hood Latches
- Safety Center-Hood Latch
- Engine Oil Filter
- Carburetor Air Cleaner
- High-Strength Door Locks*
- Two-Key Locking System*
- Safety Parked Instrument Panel*
- Pop-In Crankcase Ventilation
- Exhaust Emission Control System
- Safety Rim Wheels
- Full-Floating Open-End Front Axle
- ABE Volvo CJ
- Subject to change without notice.

REGISTERS TRADEMARK

the order

Executive Order 14028 - 2021

The executive order will impact companies that supply IT products and services to the US government. It spells out the requirements and directives mandatory for all critical software sold to the US government.

Executive Order 14028

May 12, 2021

Sec. 4. Enhancing Software Supply Chain Security.

(e) ... guidance shall include standards, procedures, or criteria regarding:

(vi) maintaining accurate and **up-to-date data, provenance (i.e., origin) of software code or components**, and controls on internal and third-party software components, tools, and services present in software development processes, **and performing audits and enforcement of these controls on a recurring basis**;

(vii) **providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website**;

(viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process;

(ix) attesting to conformity with secure software development practices; and

(x) **ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product.**

(f) Within 60 days of the date of this order, the Secretary of Commerce, in coordination with the Assistant Secretary for Communications and Information and the Administrator of the National Telecommunications and Information Administration, shall publish **minimum elements for an SBOM.**

Nutrition Facts

Serving Size 3 oz. (85g)
Serving Per Container 2

Amount Per Serving		Calories from Fat 120
Calories	200	% Daily Value

Total Fat 15g

Saturated Fat 5g

Trans Fat 3g

Cholesterol 30mg

Sodium 650mg

Total Carbohydrate 30g

Dietary Fiber 0g

Sugars 5g

Protein 5g

Vitamin A 5%

Calcium 15%

Vitamin C 2%

Iron 5%

*Percent Daily Values are based on a 2,000 calorie diet.
Your Daily Values may be higher or lower depending on your calorie needs.

Total Fat	Less than	2,000	2,500
Total Fat	Less than	65g	80g
Total Fat	Less than	20g	25g
Total Fat	Less than	300mg	300mg
Total Fat	Less than	2,400mg	2,400mg
Total Fat	Less than	300mg	375mg
Total Fat	Less than	2,400mg	300mg

**FORTIFIED
WITH LOG4J!**



Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.

No provenance, integrity or
license information in the
minimum requirements?

A young boy with short brown hair and a sad, pouting expression. He is wearing a bright yellow t-shirt with a circular sticker that says "Don't Waste!". The background is plain white.

No proven integrity or
license information in the
minimum requirements?

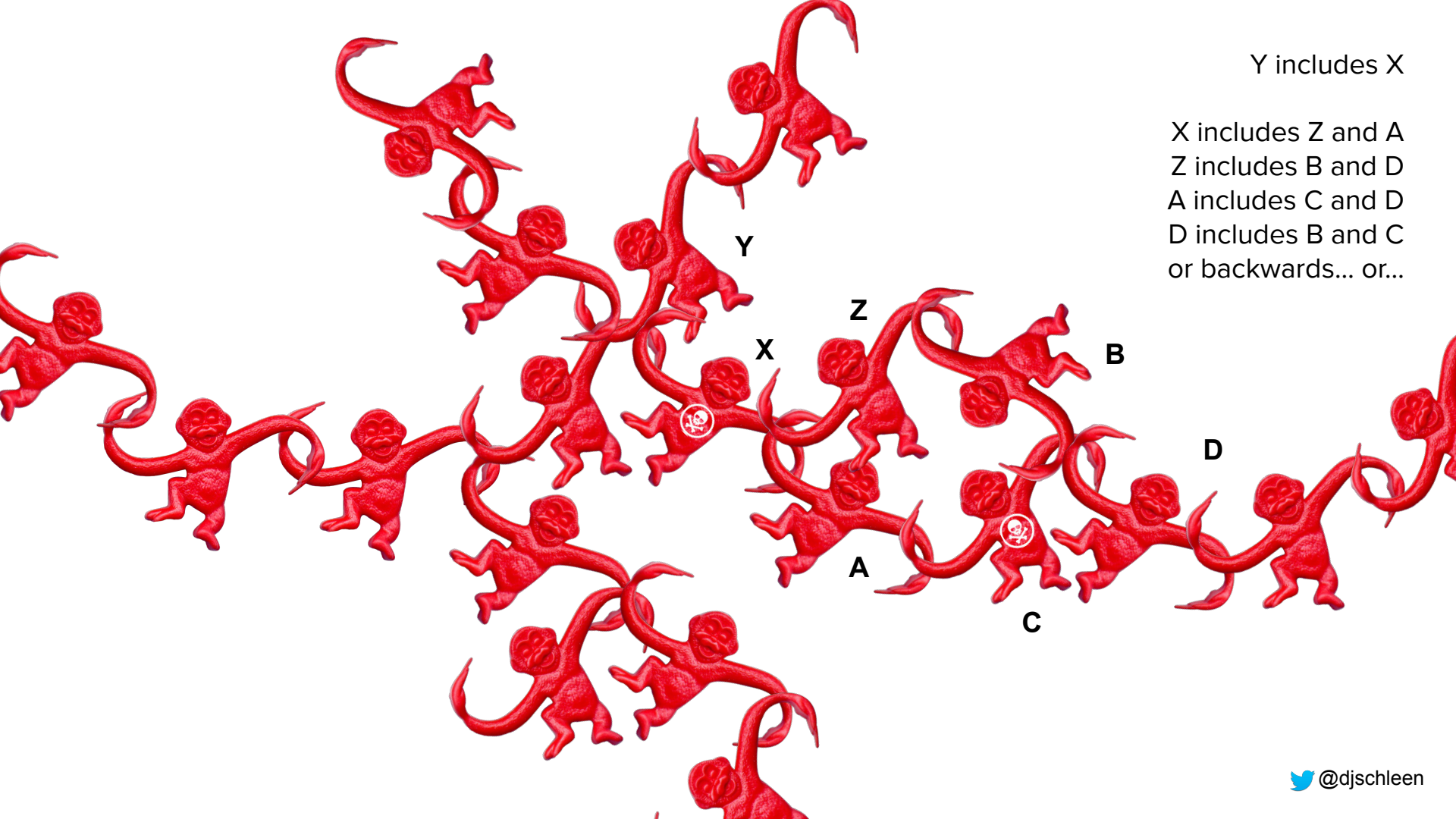
REALLY?



Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.

A close-up photograph of a red metal chain, likely made of cast iron or steel, with a textured surface. The chain is draped across the frame, with some links in sharp focus and others blurred in the background. The text "supply chain" is overlaid in a large, bold, grey sans-serif font, centered horizontally and partially obscured by the chain's links.

supply chain



Y includes X

X includes Z and A
Z includes B and D
A includes C and D
D includes B and C
or backwards... or...

Y

X

Z

B

D

A

C



Y includes X

X includes Z and A

Z includes B and D

A includes C and D

D includes B and C
or backwards... or...

MONKEYS!

B

D

C

12

Direct
References



16

Indirect
References



```
go.mod
Run go mod tidy | Create vendor directory
1  module github.com/devops-kung-fu/bomber
2
3  go 1.19
4
Check for upgrades | Upgrade transitive dependencies | Upgrade direct dependencies
5  require (
6      github.com/CycloneDX/cyclonedx-go v0.7.0
7      github.com/briandowns/spinner v1.19.0
8      github.com/devops-kung-fu/common v0.2.5
9      github.com/gookit/color v1.5.2
10     github.com/jarcoal/httpmock v1.2.0
11     github.com/jedib0t/go-pretty/v6 v6.4.0
12     github.com/kirinlabs/HttpRequest v1.1.1
13     github.com/package-url/packageurl-go v0.1.0
14     github.com/spf13/afero v1.9.2
15     github.com/spf13/cobra v1.5.0
16     github.com/stretchr/testify v1.8.0
17     k8s.io/utils v0.0.0-20220922133306-665eaec4324
18 )
19
20 require (
21     github.com/davecgh/go-spew v1.1.1 // indirect
22     github.com/fatih/color v1.13.0 // indirect
23     github.com/inconshreveable/mousetrap v1.0.1 // indirect
24     github.com/kr/text v0.2.0 // indirect
25     github.com/mattn/go-colorable v0.1.13 // indirect
26     github.com/mattn/go-isatty v0.0.16 // indirect
27     github.com/mattn/go-runewidth v0.0.14 // indirect
28     github.com/niemeyer/pretty v0.0.0-20200227124842-a10e7caefd8e // indirect
29     github.com/pmezard/go-difflib v1.0.0 // indirect
30     github.com/rivo/uniseg v0.4.2 // indirect
31     github.com/spf13/pflag v1.0.5 // indirect
32     github.com/xo/terminfo v0.0.0-20220910002029-abceb7e1c41e // indirect
33     golang.org/x/sys v0.0.0-20220928140112-f11e5e49a4ec // indirect
34     golang.org/x/text v0.3.7 // indirect
35     gopkg.in/check.v1 v1.0.0-20200227125254-8fa46927fb4f // indirect
36     gopkg.in/yaml.v3 v3.0.1 // indirect
37 )
38
```

☰ go.sum

```
478 google.golang.org/grpc v1.34.0/go.mod h1:Wotjhfg0W/P0jDeRt8vscBtXq+2Vj0RFy659qA51WJ8=
479 google.golang.org/grpc v1.35.0/go.mod h1:qjiiYl8FncCW8fEJPdyg3v6XW24KsRHe+dy9BAGRRJU=
480 google.golang.org/protobuf v0.0.0-20200109180630-ec00e32a8dfd/go.mod h1:DFci5gLYBciE7Vtevhsrf46CRTquxDuW5QurQQe4oz8=
481 google.golang.org/protobuf v0.0.0-20200221191635-4d8936d0db64/go.mod h1:kwYJMbJ01WoiD6+Kah6886xMzcty6N08ah7+eCXa0=
482 google.golang.org/protobuf v0.0.0-20200228230310-ab0ca4ff8a60/go.mod h1:cftL7dwQJ+fmap5saPgwCLgHXTUD7jkjRqWcaiX5VYM=
483 google.golang.org/protobuf v1.20.1-0.20200309200217-e05f789c0967/go.mod h1:A+miEFZTKqfCUM6K7xSMQL90KL/b6hQv+e19PK+JZNE=
484 google.golang.org/protobuf v1.21.0/go.mod h1:47Nbq4nVaFHyn7iLmalzf03qCViNmQZ2kzikPIcrTAo=
485 google.golang.org/protobuf v1.22.0/go.mod h1:EGpADcykh3NcUnDUJcl1+ZksZNG860LYog2L/sGQquU=
486 google.golang.org/protobuf v1.23.0/go.mod h1:EGpADcykh3NcUnDUJcl1+ZksZNG860LYog2L/sGQquU=
487 google.golang.org/protobuf v1.23.1-0.20200526195155-81db48ad09cc/go.mod h1:EGpADcykh3NcUnDUJcl1+ZksZNG860LYog2L/sGQquU=
488 google.golang.org/protobuf v1.24.0/go.mod h1:r/3tXBNzIEhYS9I0UvjXDlt8tc493IDkGjtUeSXeh4=
489 google.golang.org/protobuf v1.25.0/go.mod h1:9JNX74DMeImyA3h4bdi1ymwjUzf21/xILbajtzgsN7c=
490 gopkg.in/check.v1 v0.0.0-20161208181325-20d25e280405/go.mod h1:Co6ibVJAznAaIkqp8huTwlJQCZ016jof/cbN4VW5Yz0=
491 gopkg.in/check.v1 v1.0.0-20180628173108-788fd7840127/go.mod h1:Co6ibVJAznAaIkqp8huTwlJQCZ016jof/cbN4VW5Yz0=
492 gopkg.in/check.v1 v1.0.0-20200227125254-8f7b211b517c/go.mod h1:BLr19bFF+O6necV7AaIwq18hcH8XK9/i0At2xKjWk4p6zsU=
493 gopkg.in/check.v1 v1.0.0-20200227125254-8f7b211b517c/go.mod h1:Co6ibVJAznAaIkqp8huTwlJQCZ016jof/cbN4VW5Yz0=
494 gopkg.in/errgo.v2 v2.1.0/go.mod h1:hNsd1EYgqzUytp96Fy3vVqL801yvfDNI=
495 gopkg.in/yaml.v2 v2.2.2/go.mod h1:hI93XBmqg5FWXqnnZvOr4Ln/zCPuaghnlEUweFUi=
496 gopkg.in/yaml.v2 v2.4.0/go.mod h1:RDklbk79AGWmwhvvtgZtapE0x6ZbXqjvGnsGnQ=
497 gopkg.in/yaml.v3 v3.0.0-20200313102051-9f26c0678c70/go.mod h1:kq4uy7z7rIzviUmN+EgEM=
498 gopkg.in/yaml.v3 v3.0.1 h1:fxVm/GzAzEWqLHuvctLSHsG+nNmmW00wduXjJY57CA=
499 gopkg.in/yaml.v3 v3.0.1/go.mod h1:K4uyk7z7BCEPqu6E+C64Yfv1cQ7kz7rIZviUmN+EgEM=
500 honnef.co/go/tools v0.0.0-20190102054323-c2f93a96b099/go.mod h1:rf3LG4BRIbNafJWhAfAdb/ePZxsR/4RtNHQocxwk9r4=
501 honnef.co/go/tools v0.0.0-20190106161140-3f1c274a020f/go.mod h1:rf3LG4BRIbNafJWhAfAdb/ePZxsR/4RtNHQocxwk9r4=
502 honnef.co/go/tools v0.0.0-20190418001031-e561f6794a2a/go.mod h1:rf3LG4BRIbNafJWhAfAdb/ePZxsR/4RtNHQocxwk9r4=
503 honnef.co/go/tools v0.0.0-20190523083050-ea95bfd59fc/go.mod h1:rf3LG4BRIbNafJWhAfAdb/ePZxsR/4RtNHQocxwk9r4=
504 honnef.co/go/tools v0.0.1-2019.2.3/go.mod h1:a3bituU0lyd329TUQxRnasdCoJdKEUEAqEt0JzvZhAg=
505 honnef.co/go/tools v0.0.1-2020.1.3/go.mod h1:X/FiERA/W4tHapMX5mGpAtMSVeeEU0yHaw9vFzvIQ3k=
506 honnef.co/go/tools v0.0.1-2020.1.4/go.mod h1:X/FiERA/W4tHapMX5mGpAtMSVeeEU0yHaw9vFzvIQ3k=
507 k8s.io/utlis v0.0.0-20220922133306-665eaec4324 h1:i+xdFemcSNUjvIFblaYuXgRondKxK4z4prVPKzEaelI=
508 k8s.io/utlis v0.0.0-20220922133306-665eaec4324/go.mod h1:0LgZIPagt7ERELqWJFomSt595RzquPNLL48i0WgY0g0=
509 rsc.io/binaryregexp v0.2.0/go.mod h1:qT7V/C0ck+e2FymRvadV62gMdZztPaShug0Ci3I+8D8=
510 rsc.io/quote/v3 v3.1.0/go.mod h1:yEA65RcK8LYaZtP9Kv3t0HmxON59tX3rD+TICJquLj0=
511 rsc.io/sampler v1.3.0/go.mod h1:T1hPZKmBbMnahiBKfy5HrXp6adAjAcjK9JXDnKaTXpA=
512
```

511

Transitive References



OWASP - 2017

NIST NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

SWID

2009, then revised in 2015.



syft

Anchore



Linux Foundation - 2010

formats



← ICS ← 35 ← 35.080

ISO/IEC 5962:2021

Information technology — SPDX® Specification V2.2.1

The electronic version of this International Standard can be **downloaded** from the ISO/IEC Information Technology Task Force (ITTF) web site.

Abstract

[Preview](#)

This Software Package Data Exchange® (SPDX®) specification defines a standard data format for communicating the component and metadata information associated with software packages. An SPDX document can be associated with a set of software packages, files or snippets and contains information about the software in the SPDX format described in this specification.

General information

Status :  Published

Publication date : 2021-08

Edition : 1

Number of pages : 145

Technical Committee : [ISO/IEC JTC 1](#) Information technology

ICS : [35.080](#) Software

Buy this standard

Format

Language

PDF

English

Paper

English

CHF 198

 Buy

standard



← ICS ← 35 ← 35.080

ISO/IEC 5962:2021 Information technology – Specification V2.2.1



The electronic version of this International Standard can be [downloaded](#) from the International Standards Information Technology Task Force (ITTF) web site.

Abstract

This Software Package Data Exchange® (SPDX®) specification defines a standard data format for communicating the component and metadata information associated with software packages. This document can be associated with a set of software packages, files or snippets and contains information about the software in the SPDX format described in this specification.

General information

Status :  Published

Publication date :

Edition : 1

Number of pages :

Technical Committee : [ISO/IEC JTC 1](#) Information technology

ICS : [35.080](#) Software

Buy this standard

Format

Language

PDF

English

Paper

English

CHF 198



REALLY?

too soon?

- Standards change and evolve quickly.
- Too many formats interoperability is suggested but non-existent
- JSON and XML isn't easily understood by the non-technical
- Generate them with every release. Now what?
- A vendor provides one. Now what?
- A vendor gets feedback from customers that their software has vulnerabilities. Now what?
- How do I search across all my SBOMs to find a specific component?
- Where to store these things?
- Conversion can be lossy
- Frequency of updates
- Distribution and Delivery
- Access Control and Privacy
- A supply chain isn't linear...

issues

what we can do



**SCA = Your Source / Open Source
(Generate)**

Releases / v0.3.3

v0.3.3

Latest

Compare

djschleen released this 6 days ago · 2 commits to main since this release

d58403d

Changelog

- d58403d feat: License support (#58)

Assets

13

bomber.spdx.json	156 KB	6 days ago
bomber_0.3.3_darwin_all.tar.gz	6.04 MB	6 days ago
bomber_0.3.3_linux_amd64.deb	3.08 MB	6 days ago
bomber_0.3.3_linux_amd64.rpm	3.08 MB	6 days ago
bomber_0.3.3_linux_amd64.tar.gz	2.98 MB	6 days ago
bomber_0.3.3_linux_arm64.deb	2.8 MB	6 days ago
bomber_0.3.3_linux_arm64.rpm	2.8 MB	6 days ago
bomber_0.3.3_linux_arm64.tar.gz	2.72 MB	6 days ago
bomber_0.3.3_windows_amd64.tar.gz	3.07 MB	6 days ago
bomber_0.3.3_windows_arm64.tar.gz	2.81 MB	6 days ago
checksums.txt	873 Bytes	6 days ago
Source code (zip)		6 days ago
Source code (tar.gz)		6 days ago

Build the functionality into your release process



? = Closed Source
(Consume)

TPRG (Third Party Risk Governance)



grype

Anchore
(Scans Containers)



Bomber
DKFM
(Scans Everything)

scan for vulnerabilities

```

● dj@dkfm ~/code/bomber (license-support) $ ./bomber scan --provider=ossindex ./sbom/test/juiceshop.cyclonedx.json

BOMBER

DKFM - DevOps Kung Fu Mafia
https://github.com/devops-kung-fu/bomber
Version: 0.3.3

A newer version of bomber is available (v0.3.2)

■ Ecosystems detected: npm
■ Scanning 840 packages for vulnerabilities...
■ Vulnerability Provider: Sonatype OSS Index (https://ossindex.sonatype.org)

■ Licenses Found: MIT, ISC, BSD-3-Clause, BSD-2-Clause, Apache-2.0, CC-BY-3.0, CC0-1.0, 0BSD, Unlicense, WTFPL

```

TYPE	NAME	VERSION	SEVERITY	VULNERABILITY
npm	y18n	4.0.0	HIGH	sonatype-2020-1040
	xmllhttprequest-ssl	1.5.5	CRITICAL	CVE-2021-31597



bomber Results

The following results were detected by **bomber 0.3.3** on 2022-09-28 16:42:05.299127-0600 MDT m+=8.502065449 using the ossindex provider. Vulnerabilities displayed may differ from provider to provider. This list may not contain all possible vulnerabilities. Please try the other providers that **bomber** supports (see [ossindex](#)). There is no guarantee that the next time you scan for vulnerabilities that there won't be more, or less of them. Threats are continuous.

Licenses

The following licenses were found by **bomber**:

- MIT
- ISC
- BSD-3-Clause
- BSD-2-Clause
- Apache-2.0
- CC-BY-3.0
- CC0-1.0
- 0BSD
- Unlicense
- WTFPL

Vulnerability Summary

Critical: 14
 High: 35
 Moderate: 23
 Low: 1
 Unspecified: 0

Vulnerability Details

pkg:npm/mout@1.2.2

Modular Utilities

Vulnerabilities

[CVE-2020-7792] CWE-471: Modification of Assumed-Immutable Data (MAID)

Severity: **HIGH**

[Reference Documentation](#)

This affects all versions of package mout. The deepFillIn function can be used to 'fill missing properties recursively', while the deepMixIn 'mixes objects into the target object, recursively mixing existing child objects as well'. In both cases, the key used to access the target object recursively is not checked, leading to a Prototype Pollution.



```

{
  "meta": {
    "generator": "bomber",
    "url": "https://github.com/devops-kung-fu/bomber",
    "version": "0.3.3",
    "provider": "ossindex",
    "date": "2022-09-27T17:16:31.760526-06:00"
  },
  "licenses": [
    "MIT",
    "ISC",
    "BSD-3-Clause",
    "BSD-2-Clause",
    "Apache-2.0",
    "CC-BY-3.0",
    "CC0-1.0",
    "0BSD",
    "Unlicense",
    "WTFPL"
  ],
  "summary": {
    "Unspecified": 0,
    "Low": 1,
    "Moderate": 23,
    "High": 35,
    "Critical": 14
  },
  "packages": [
    {
      "coordinates": "pkg:npm/mout@1.2.2",
      "reference": "https://ossindex.sonatype.org/co",
      "description": "Modular Utilities",
      "vulnerabilities": [
        {
          "id": "CVE-2020-7792",
          "displayName": "CVE-2020-7792"
        }
      ]
    }
  ]
}

```

bomber output

- Generate and include SBOMs as an artifact with every release
- Request SBOMs from your vendors when doing security reviews (TPRG)
- Scan closed-source SBOMs for Security Vulnerabilities
- Store SBOMs in a shared artifact repository with appropriate access controls and update often
- Work with your vendors when you find vulnerabilities.
- Realize that we are early in the SBOM world. Everyone is still trying to figure out the landscape.

parting words

THANK YOU!

DJ Schleen

Distinguished Security Architect - Paranoids @ Yahoo

 @djschleen

