Software Barrel of Monkeys (SBOM)

DJ Schleen

Distinguished Security Architect - Paranoids @ Yahoo

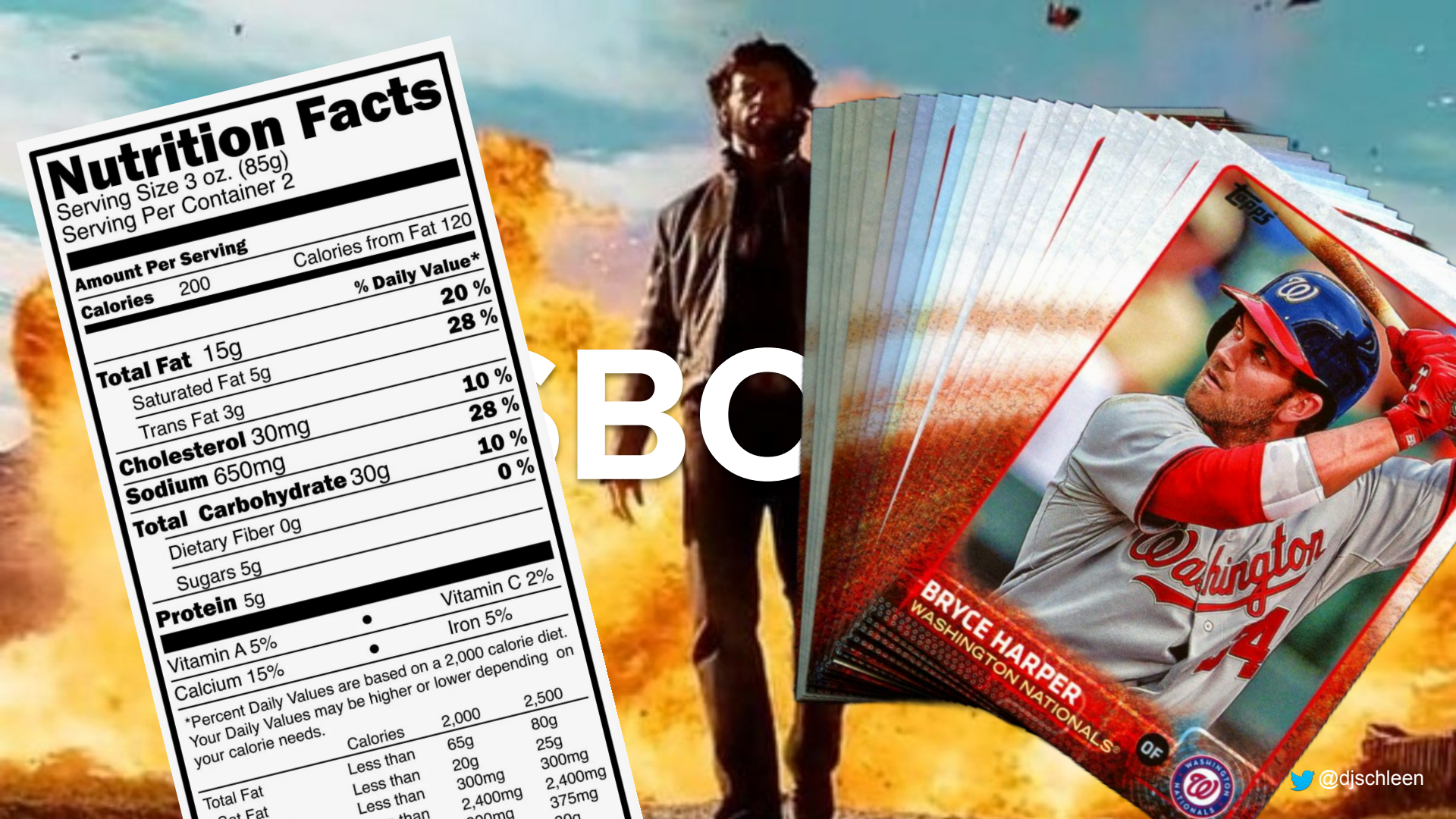
@djschleen

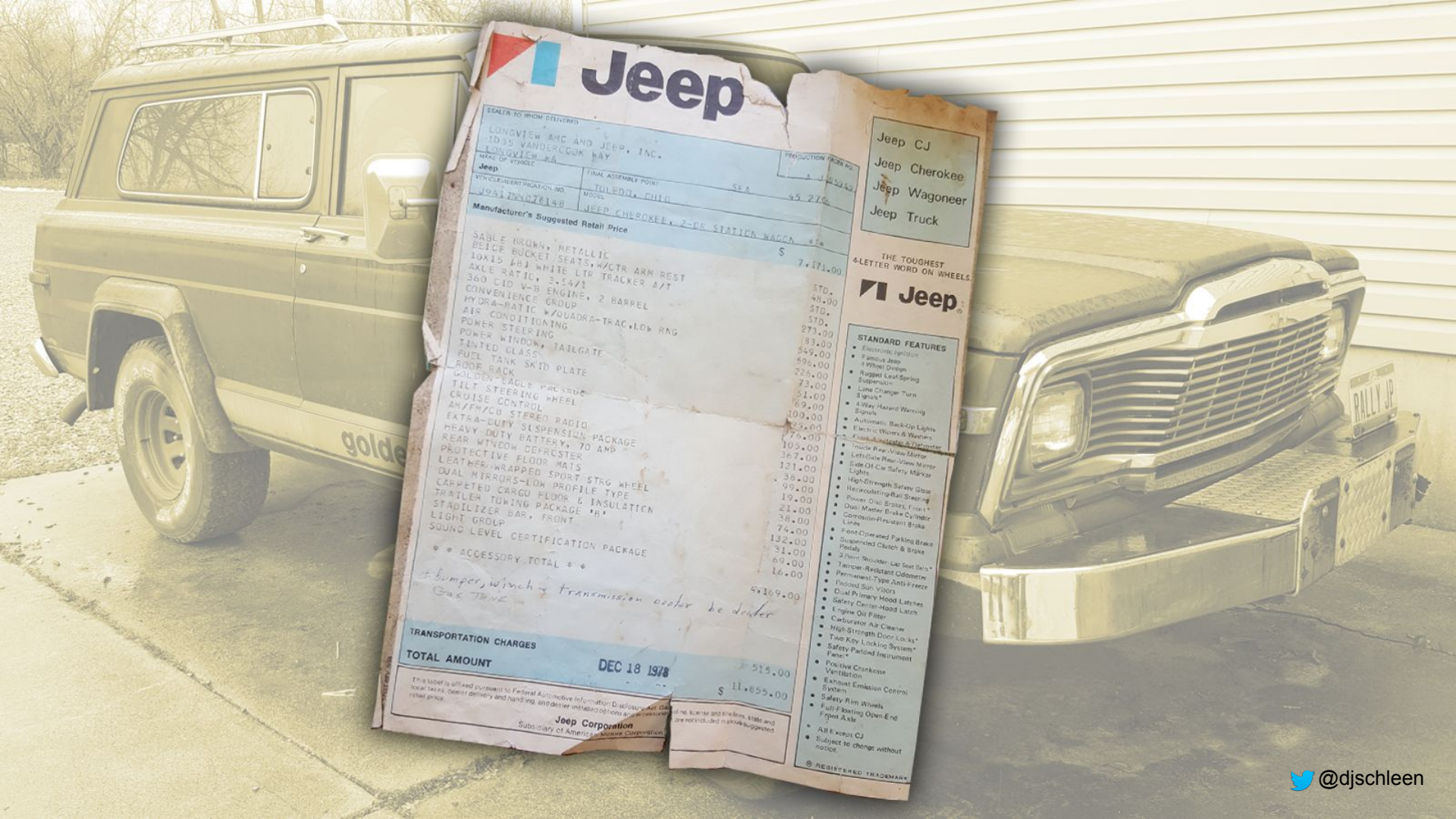

openssl story

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

WHERE IS IT?


SBOM
@djschleen

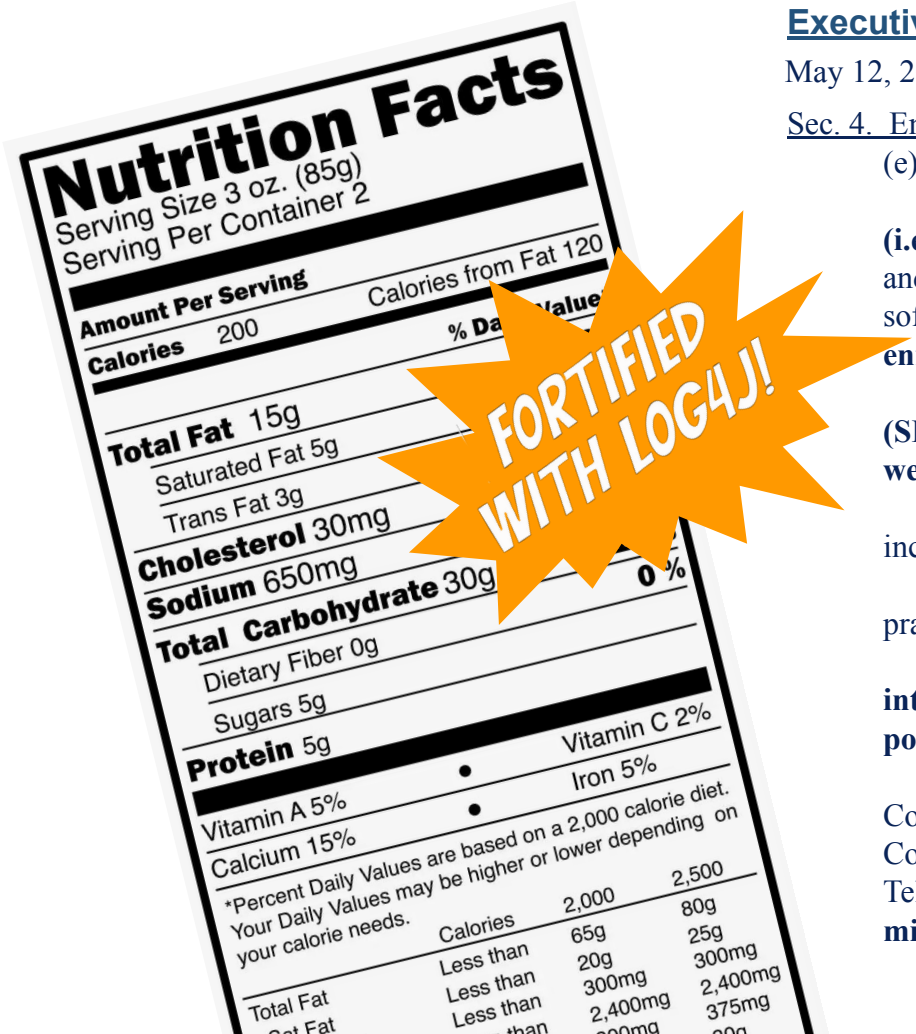

Nutrition Facts
Serving Size 3 oz. (85g)
Serving Per Container 2
Amount Per Serving
Calories 200
Calories from Fat 120
% Daily Value*
Total Fat 15g 20 %
Saturated Fat 5g 28 %
Trans Fat 3g
Cholesterol 30mg 10 %
Sodium 650mg 28 %
Total Carbohydrate 30g 10 %
Dietary Fiber 0g 0 %
Sugars 5g
Protein 5g
Vitamin 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
Less than 20g 25g
Less than 300mg 300mg
2,400mg 2,400mg
than 375mg
BRYCE HARPER
WASHINGTON NATIONALS
OF
Washington
@djschleen


Jeep
DEALER TO WHOM DELIVERED
LONGVIEW AMC AND JEEP, INC.
1035 VANDERCOOK WAY
LONGVIEW, WA
MAKE OF VEHICLE
Jeep
VEHICLE IDENTIFICATION NO.
J9A1NW078148
FINAL ASSEMBLY POINT
TOLEDO, OHIO
MODEL
JEEP CHEROKEE, 2-DR STATION WAGON 4x4
Manufacturer's Suggested Retail Price
$ 7,171.00
SABLE BROWN, METALLIC
BEIGE BUCKET SEATS, W/CTR ARM REST
10x15 AB1 WHITE LTR TRACKER A/T
AXLE RATIO, 3.54/1
360 CID V-8 ENGINE, 2 BARREL
CONVENIENCE GROUP
HYDRA-MATIC W/QUADRA-TRAC, LOW RNG
AIR CONDITIONING
POWER STEERING
POWER WINDOW, TAILGATE
TINTED GLASS
FUEL TANK SKID PLATE
ROOF RACK
GOLDEN EAGLE PACKAGE
TILT STEERING WHEEL
CRUISE CONTROL
AM/FM/CB STEREO RADIO
EXTRA-DUTY SUSPENSION PACKAGE
HEAVY DUTY BATTERY, 70 AMP
REAR WINDOW DEFROSTER
PROTECTIVE FLOOR MATS
LEATHER-WRAPPED SPORT STRG WHEEL
DUAL MIRRORS-LOW PROFILE TYPE
CARPETED CARGO FLOOR & INSULATION
TRAILER TOWING PACKAGE "B"
STABILIZER BAR, FRONT
LIGHT GROUP
SOUND LEVEL CERTIFICATION PACKAGE
** ACCESSORY TOTAL **
4,169.00
#bumper, winch, transmission cooler to dealer
Gas Tank
TRANSPORTATION CHARGES
515.00
TOTAL AMOUNT
DEC 18 1978
$ 11,855.00
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
Famous Jeep 4-Wheel Design
Rugged Leaf-Spring Suspension
Lane Changer Turn Signals*
4-Way Hazard Warning Signals
Automatic Back-Up Lights
Electric Wipers & Washers
Trucks Have Tachometer
Inside Rear-View Mirror
Left-Side Rear-View Mirror
Side-Of-Car Safety Marker Lights
High-Strength Safety Glass
Recirculating-Ball Steering
Power Disc Brakes, Front*
Dual Master Brake Cylinder
Corrosion-Resistant Brake Lines
Foot-Operated Parking Brake
Suspended Clutch & Brake Pedals
3-Point Shoulder-Type Seat Belts*
Tamper-Resistant Odometer
Permanent-Type Anti-Freeze
Padded 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-Padded Instrument Panel*
Positive Crankcase Ventilation
Exhaust Emission Control System
Safety-Rim Wheels
Full-Floating Open-End Front Axle
* All Except CJ
Subject to change without notice.
® REGISTERED TRADEMARK
golde
RALLY JP

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.**

@djschleen

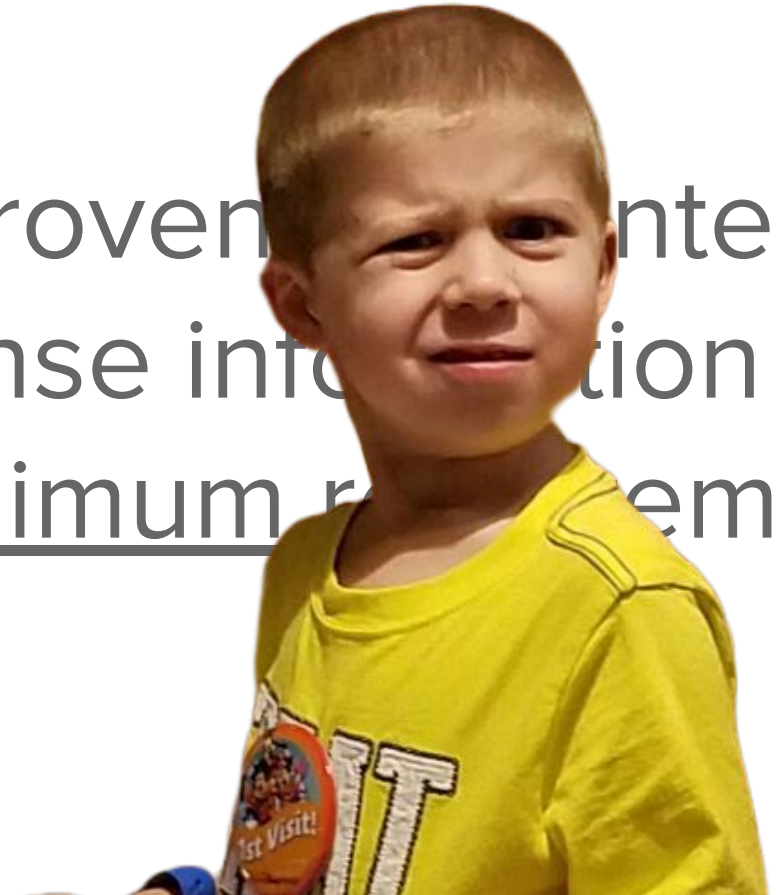
Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously 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.

https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

@djschleen

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

No proven[illegible]ntegrity or license info[illegible]tion in the minimum r[illegible]ements?



REALLY?

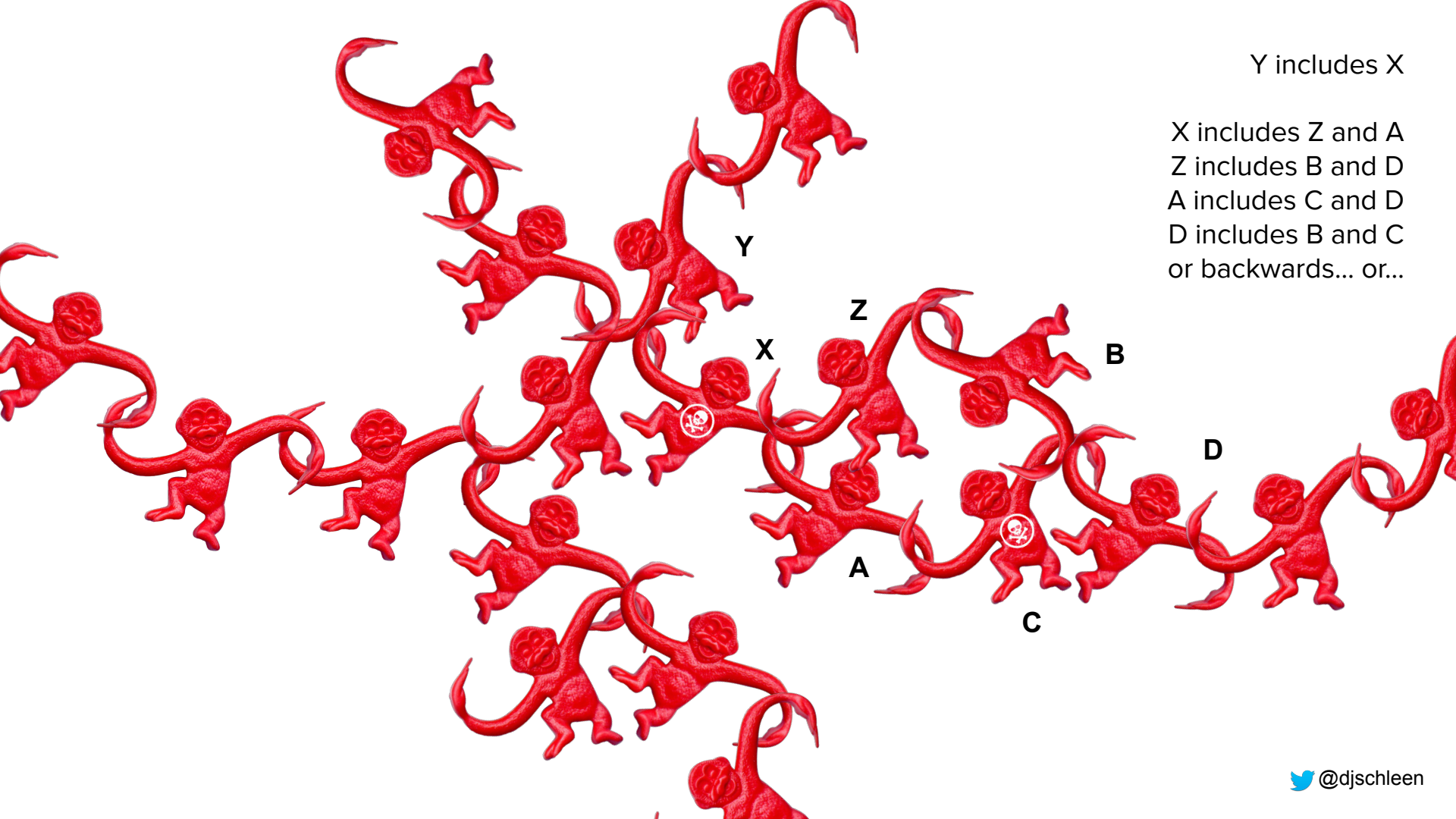
@djschleen

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.

https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

@djschleen


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...

@djschleen

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!

@djschleen

12

Direct References

16

Indirect References

go.sum

```
google.golang.org/grpc v1.34.0/go.mod h1:WotjhfgOW/POjDeRt8vscBtXq+2VjORFy659qA51WJ8=
google.golang.org/grpc v1.35.0/go.mod h1:qjiiYl8FncCW8feJPdyg3v6XW24KsRHe+dy9BAGRRjU=
google.golang.org/protobuf v0.0.0-20200109180630-ec00e32a8dfd/go.mod h1:DFci5gLYBciE7Vtevhsrf46CRTquxDuWsQurQQe4oz8=
google.golang.org/protobuf v0.0.0-20200221191635-4d8936d0db64/go.mod h1:kwYJMbMJ01Woi6D6+Kah6886xMZcty6N08ah7+eCXa0=
google.golang.org/protobuf v0.0.0-20200228230310-ab0ca4ff8a60/go.mod h1:cfTl7dwQJ+fmap5saPgwCLgHXTUD7jkjRqWcaiX5VyM=
google.golang.org/protobuf v1.20.1-0.20200309200217-e05f789c0967/go.mod h1:A+miEFZTKqfCUM6K7xSMQL9OKL/b6hQv+e19PK+JZNE=
google.golang.org/protobuf v1.21.0/go.mod h1:47Nbq4nVaFHyn7ilMalzfO3qCViNmqZ2kzikPIcrTAo=
google.golang.org/protobuf v1.22.0/go.mod h1:EGpADcykh3NcUnDUJcl1+ZksZNG86OlYog2l/sGQquU=
google.golang.org/protobuf v1.23.0/go.mod h1:EGpADcykh3NcUnDUJcl1+ZksZNG86OlYog2l/sGQquU=
google.golang.org/protobuf v1.23.1-0.20200526195155-81db48ad09cc/go.mod h1:EGpADcykh3NcUnDUJcl1+ZksZNG86OlYog2l/sGQquU=
google.golang.org/protobuf v1.24.0/go.mod h1:r/3tXBNzIEhYS9I1OUVjXDlt8tc493IdKGjtUeSXeh4=
google.golang.org/protobuf v1.25.0/go.mod h1:9JNX74DMeImyA3h4bdi1ymwjUzf21/xIlbajtzgsN7c=
gopkg.in/check.v1 v0.0.0-20161208181325-20d25e280405/go.mod h1:Co6ibVJAznAaIkqp8huTwlJQCZ016jof/cbN4VW5Yz0=
gopkg.in/check.v1 v1.0.0-20180628173108-788fd7840127/go.mod h1:Co6ibVJAznAaIkqp8huTwlJQCZ016jof/cbN4VW5Yz0=
gopkg.in/check.v1 v1.0.0-20200227125254-8f
gopkg.in/check.v1 v1.0.0-20200227125254-8f
gopkg.in/errgo.v2 v2.1.0/go.mod h1:hNsd1EY
gopkg.in/yaml.v2 v2.2.2/go.mod h1:hI93XBmq
gopkg.in/yaml.v2 v2.4.0/go.mod h1:RDklbk79AGWmwhnv
gopkg.in/yaml.v3 v3.0.0-20200313102051-9f2
gopkg.in/yaml.v3 v3.0.1 h1:fxVm/GzAzEWqLHuvct
gopkg.in/yaml.v3 v3.0.1/go.mod h1:K4uyk7z7BCEPqu6E+C64Yfv1cQ7kz7rIZviUmN+EgEM=
honnef.co/go/tools v0.0.0-20190102054323-c2f93a96b099/go.mod h1:rf3lG4BRIbNafJWhAfAdb/ePZxsR/4RtNHQocxwk9r4=
honnef.co/go/tools v0.0.0-20190106161140-3f1c8
honnef.co/go/tools v0.0.0-20190418001031-e561f6794a2a/go.mod h1:rf3lG4BRIbNafJWhAfAdb/ePZxsR/4RtNHQocxwk9r4=
honnef.co/go/tools v0.0.0-20190523083050-ea95bdfd59fc/go.mod h1:rf3lG4BRIbNafJWhAfAdb/ePZxsR/4RtNHQocxwk9r4=
honnef.co/go/tools v0.0.1-2019.2.3/go.mod h1:a3bituU0lyd329TUQxRnasdCoJDkEUEAqEt0JzvZhAg=
honnef.co/go/tools v0.0.1-2020.1.3/go.mod h1:X/FiERA/W4tHapMX5mGpAtMSVEeEUOyHaw9vFzvIQ3k=
honnef.co/go/tools v0.0.1-2020.1.4/go.mod h1:X/FiERA/W4tHapMX5mGpAtMSVEeEUOyHaw9vFzvIQ3k=
k8s.io/utils v0.0.0-20220922133306-665eaaec4324 h1:i+xdFemcSNuJvIfBlaYuXgRondKxK4z4prVPKzEaelI=
k8s.io/utils v0.0.0-20220922133306-665eaaec4324/go.mod h1:OLgZIPagt7ERELqWJFomSt595RzquPNLL48iOWgYOg0=
rsc.io/binaryregexp v0.2.0/go.mod h1:qTv7/COck+e2FymRvadv62gMdZztPaShugOCi3I+8D8=
rsc.io/quote/v3 v3.1.0/go.mod h1:yEA65RcK8LyAZtP9Kv3t0HmxON59tX3rD+tICJqUlj0=
rsc.io/sampler v1.3.0/go.mod h1:T1hPZKmBbMNahiBKFy5HrXp6adAjACjK9JXDnKaTXpA=
```

511

Transitive References

@djschleen

OWASP - 2017

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

SWID

2009, then revised in 2015.

Anchore

Linux Foundation - 2010

formats

@djschleen

← 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

standard

Standards About us News Taking part **Store** Search

← ICS ← 35 ← 35.080

ISO/IEC 5962:2021

Information technology – cification V2.2.1

The electronic version of this International Standard can be downloaded
Technology Task Force (ITTF) web site.

Abstract

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

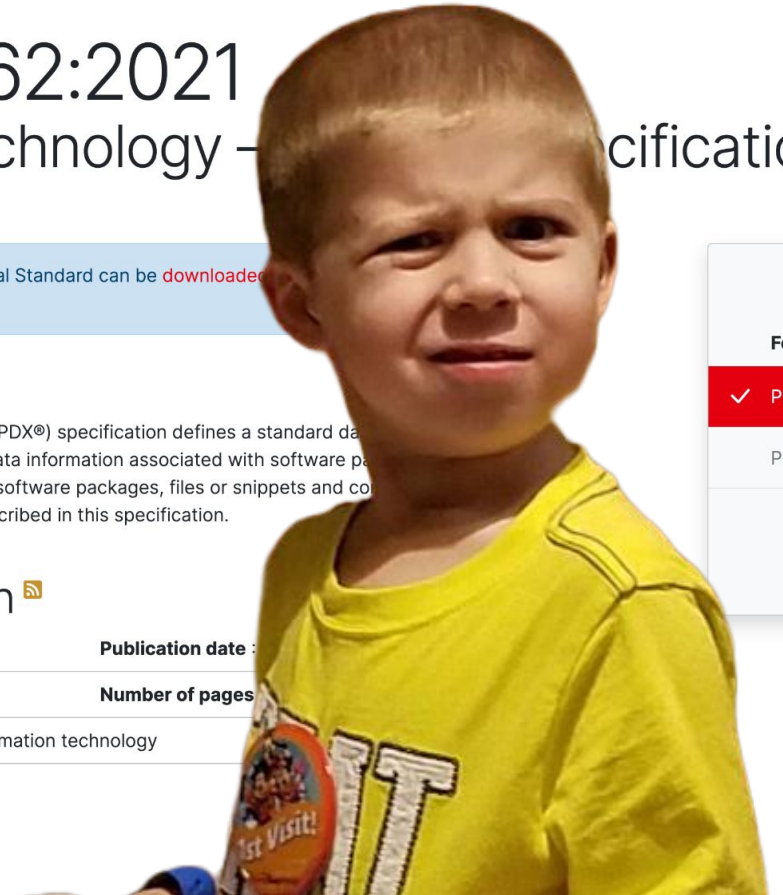
General information

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 Buy

REALLY?

djschleen

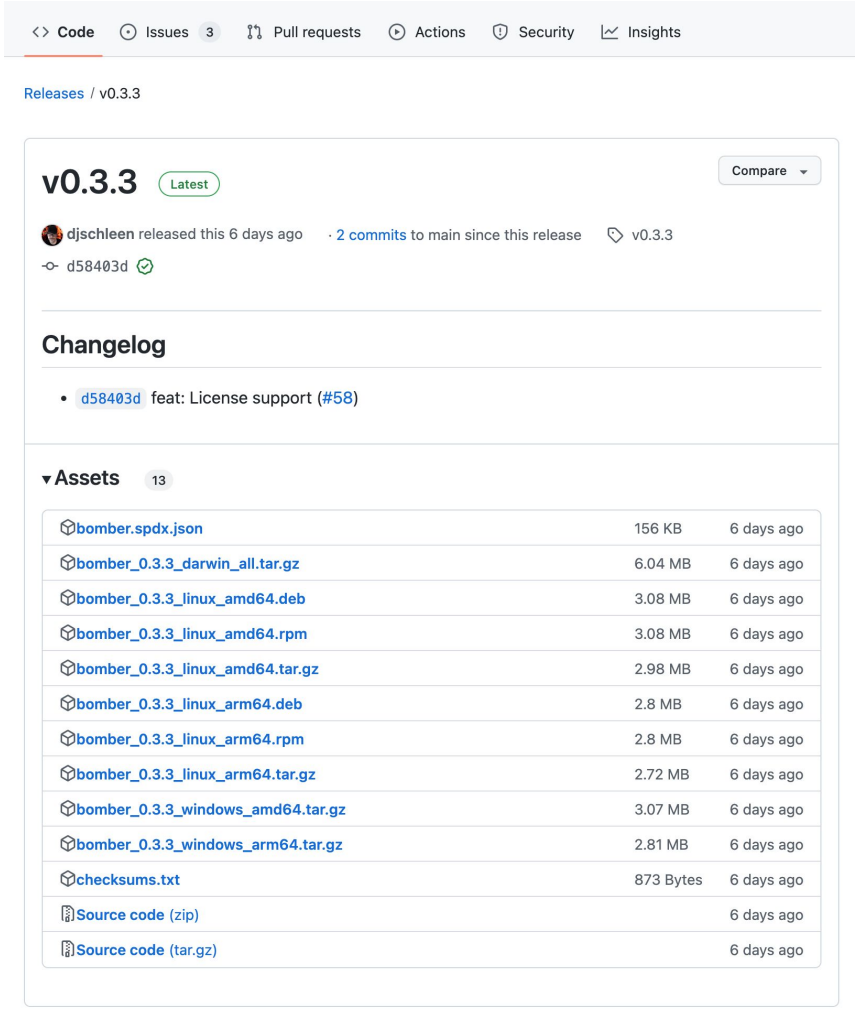
too soon?

- 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)
@djschleen



Build the functionality into your release process

@djschleen


? = Closed Source
(Consume)
@djschleen

TPRG (Third Party Risk Governance)

Anchore
(Scans Containers)

Bomber
DKFM
(Scans Everything)

scan for vulnerabilities

bomber output

```
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
	xmlhttprequest-ssl	1.5.5	CRITICAL	CVE-2021-31597


```
{
        "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 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 (osv, 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.

https://github.com/devops-kung-fu/bomber

@djschleen

- 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

@djschleen

THANK YOU!

DJ Schleen

Distinguished Security Architect - Paranoids @ Yahoo

@djschleen