



Evolving vulnerabilities in CycloneDX

Gareth Rushgrove



Gareth Rushgrove

VP Products, Snyk

Devops Weekly curator

Conftest/Open Policy Agent maintainer

Open Source contributor

@garethr

Agenda

01 CycloneDX introduction

02 Vulnerability extension improvements

03 Next steps



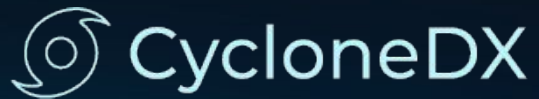
CycloneDX

Very quick introduction

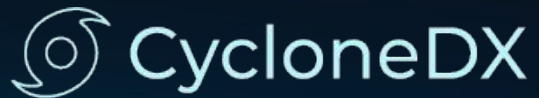


CycloneDX is a lightweight software bill of materials (SBOM) standard designed for use in application security contexts and supply chain component analysis.

- Originally extracted from OWASP Dependency-Track
- Open specification
- Open Source under Apache 2.0
- Tools for generating SBoMs for Maven, Gradle, .NET, Node, Rust, Python, PHP, Ruby and Cocoapods
- cyclonedx.org and github.com/CycloneDX



- Define a vendor agnostic specification independent of language or ecosystem
- Specification should be machine readable
- Specification should be easy to implement with minimal effort
- Specification should be simple and performant to parse
- Specification should provide lightweight schema definitions for JSON and XML
- Specification should reuse parts of existing specs where beneficial
- **Specification should be extensible to support specialized and future use cases**
- Specification should be decentralized, authoritative, and security focused
- Specification should promote continuous component analysis
- Should support hardware, libraries, frameworks, applications, containers, and operating systems



```
<?xml version="1.0" encoding="UTF-8"?>
<bom xmlns="http://cyclonedx.org/schema/bom/1.2"
serialNumber="urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79" version="1">
  <components>
    <component type="library">
      <publisher>Apache</publisher>
      <group>org.apache.tomcat</group>
      <name>tomcat-catalina</name>
      <version>9.0.14</version>
      <hashes>
        <hash alg="MD5">3942447fac867ae5cdb3229b658f4d48</hash>
        <hash alg="SHA-1">e6b1000b94e835ffd37f4c6dcbdad43f4b48a02a</hash>
        <hash
alg="SHA-256">f498a8ff2dd007e29c2074f5e4b01a9a01775c3ff3aeaf6906ea503bc5791b7b</hash>
        <hash
alg="SHA-512">e8f33e424f3f4ed6db76a482fde1a5298970e442c531729119e37991884bdfbfab4f9426b7ee11fccd07
4eeda0634d71697d6f88a460dce0ac8d627a29f7d1282</hash>
      </hashes>
      <licenses>
        <license>
          <id>Apache-2.0</id>
        </license>
      </licenses>
      <purl>pkg:maven/org.apache.tomcat/tomcat-catalina@9.0.14</purl>
    </component>
    <!-- More components here -->
  </components>
</bom>
```



```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.2",
  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
  "version": 1,
  "components": [
    {
      "type": "library",
      "publisher": "Apache",
      "group": "org.apache.tomcat",
      "name": "tomcat-catalina",
      "version": "9.0.14",
      "hashes": [
        {
          "alg": "MD5",
          "content": "3942447fac867ae5cdb3229b658f4d48"
        },
        {
          "alg": "SHA-1",
          "content": "e6b1000b94e835ffd37f4c6dcdbdad43f4b48a02a"
        },
        {
          "alg": "SHA-256",
          "content": "f498a8ff2dd007e29c2074f5e4b01a9a01775c3ff3aeaf6906ea503bc5791b7b"
        },
        {
          "alg": "SHA-512",
```



Evolving vulnerabilities

Data modelling and suggested improvements

Vulnerability extension

Adds **.vulnerabilities** property
to CycloneDX SBOM

182 lines (182 sloc) | 6.23 KB

Raw

Blame



```
1 {
2   "$schema": "http://json-schema.org/draft-07/schema#",
3   "$id": "http://cyclonedx.org/schema/ext/vulnerability-1.0-SNAPSHOT.schema.json",
4   "type": "object",
5   "title": "CycloneDX Vulnerability Extension",
6   "$comment": "CycloneDX Vulnerability Extension for JSON Schema is published under the terms of the Apache License 2.0.",
7   "properties": {
8     "vulnerabilities": {
9       "$id": "#/properties/vulnerabilities",
10      "type": "array",
11      "items": {"$ref": "#/definitions/vulnerability"},
12      "title": "Vulnerabilities",
13      "description": "Defines a list of vulnerabilities."
14    }
15  },
16  "definitions": {
17    "cwe": {
18      "type": "integer",
19      "description": "CWE ID"
20    }
21  }
22 }
```

Example vulnerability data in CycloneDX

```
"vulnerabilities": [  
  {  
    "ref": bom-ref,  
    "id": "CVE-2010-0928",  
    "source": {  
      "name": "Snyk Intel",  
      "url": "https://snyk.io/vuln/SNYK-DEBIAN9-OPENSSL-374995"  
    },  
    "ratings": [  
      {  
        "score": {  
          "base": 9.8,  
          "impact": 5.9,  
          "exploitability": 3.0  
        },  
        "severity": "Medium",  
        "method": "CVSSv3",  
        "vector": "CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N"  
      }  
    ],  
    "cwes": [  
      310  
    ],  
    "description": "...",  
    "advisories": [  
      "https://security-tracker.debian.org/tracker/CVE-2010-0928",  
      "http://rdist.root.org/2010/03/08/attacking-rsa-exponentiation-with-fault-injection/",  
      "http://www.eecs.umich.edu/%7Evaleria/research/publications/DATE10RSA.pdf",  
      "http://www.networkworld.com/news/2010/030410-rsa-security-attack.html",  
    ]  
  }  
]
```

Vulnerabilities are complex

Real world vulnerability data comes in
lots of shapes and sizes

CycloneDX / specification

Watch 14 Star 51 Fork 11

Code Issues 9 Pull requests 1 Discussions Actions Security Insights

Discussion of vulnerability schema #38

Edit New issue

Open garethr opened this issue on 13 Oct 2020 · 17 comments



garethr commented on 13 Oct 2020



Thanks for creating the JSON Schema variant of the vulnerability extension. This prompted me to take a run at describing some real world data using the format. Here's the full example <https://gist.github.com/garethr/7dcc9d6ef4e7cc497e018dc279c00123> (bias warning, I work for Snyk, so I used Snyk in the comparison. I don't think any of the following is Snyk specific though, more about the general complexity of the domain and general usage of the output.)

Assignees

No one assigned

Labels

None yet

SUGGESTING

Support for sources on ratings

```
{
  "score": {
    "base": 9.8,
    "impact": 5.9,
    "exploitability": 3.0
  },
  "severity": "Medium",
  "source": "NVD",
  "method": "CVSSv3",
  "vector": "CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N"
},
{
  "severity": "None",
  "source": "Debian Security Tracker",
  "method": "Other"
},
{
  "score": 100,
  "severity": "Low",
  "source": "Snyk",
  "method": "Other"
}
```

SUGGESTING

Support multiple sources

```
"sources": [  
  {  
    "name": "Debian Security Tracker",  
    "url": "https://security-tracker.debian.org/tracker/CVE-2010-0928"  
  },  
  {  
    "name": "NVD",  
    "url": "https://nvd.nist.gov/vuln/detail/CVE-2010-0928"  
  }  
]
```

SUGGESTING

Arbitrary scores as well as complex CVSS

```
{
  "score": {
    "base": 9.8,
    "impact": 5.9,
    "exploitability": 3.0
  },
  "severity": "Medium",
  "source": "NVD",
  "method": "CVSSv3",
  "vector": "CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N"
},
{
  "score": 100,
  "severity": "Low",
  "source": "Snyk",
  "method": "Other"
}
```

SUGGESTING

Structured data for advisories

```
"advisories": [  
  {"url": "http://rdist.root.org/2010/03/08/attacking-rsa-exponentiation-with-fault-injection/"},  
  {"url": "http://www.eecs.umich.edu/%7Evaleria/research/publications/DAT10RSA.pdf"},  
  {"url": "http://www.networkworld.com/news/2010/030410-rsa-security-attack.html"},  
  {"url": "http://www.osvdb.org/62808"},  
  {"url": "http://www.theregister.co.uk/2010/03/04/severe_openssl_vulnerability/"},  
  {"url": "http://xforce.iss.net/xforce/xfdb/56750"},  
  {"url": "https://exchange.xforce.ibmcloud.com/vulnerabilities/56750"}  
]
```



Conclusion

Next steps and getting involved

Feedback

I'd love feedback on the open PR

Proposed evolution of the vulnerability schema for discussion #44

[Edit](#)[Open with](#) 

 **Draft** [garethr](#) wants to merge 4 commits into [CycloneDX:master](#) from [garethr:vulnerability](#) 

 Conversation **2**

 Commits **4**

 Checks **1**

 Files changed **1**

+235 -0 



[garethr](#) commented 14 days ago



WIP based on discussions in [#38](#)

- More prescriptive definition for advisories
- Support multiple sources for each vulnerability
- Allow ratings to have a named source

I've started with the JSON Schema just to iterate on ideas and get feedback. Would update examples and XSD and other parts before moving out of draft.

Reviewers

No reviews

Assignees

No one assigned

Labels

[proposed schema extension](#)

Experiment

Lots of tools to try out
and contribute to

 **Repositories** 23  Packages  People 2  Projects

Pinned repositories

specification

Software Bill-of-Material (SBOM) specification designed for use in application security contexts and supply chain component analysis

 XSLT  51  11

cyclonedx-dotnet

Creates CycloneDX Software Bill-of-Materials (SBOM) from .NET Projects

 C#  28  17

cyclonedx-maven-plugin

Creates CycloneDX Software Bill-of-Materials (SBOM) from Maven projects

 Java  38  17

cyclonedx-node-module

Creates CycloneDX Software Bill-of-Materials (SBOM) from Node.js projects

 JavaScript  29  22

cyclonedx-python

Creates CycloneDX Software Bill-of-Materials (SBOM) from Python projects

 Python  19  18

cyclonedx-cli

Preview version of the CycloneDX CLI tool

 C#  6  2

Discuss

Join in at groups.io/g/CycloneDX
and cyclonedx.org/slack/invite



Home



Subscription



Messages



Hashtags



New Topic



New Poll



Chats



Calendar



Photos



Files

[CycloneDX@groups.io](#) / Messages

Messages

Search



Msg #

Date 1 - 20 of 94



[.NET libraries v1 released](#)

Hi everyone, We've had .NET libraries available for a little while now but the first v1 has been released on NuGet. They've been in use by the .NET and CLI tools for a while now. But the public
By Patrick Dwyer (coderpatros) · #94 · 12/21/20

[CycloneDX CLI Tool New Features](#)

Hi everyone, The CLI tool has a couple of new features. The first is the analyze command which currently reports on components that have been included in an SBOM multiple times with different
By Patrick Dwyer (coderpatros) · #93 · 12/21/20

[CycloneDX CLI Tool](#)

As some of you would be aware we have a CycloneDX CLI tool available now. Initial effort has been on full specification version support. As well as being able to produce SPDX format SBOMs from
By Patrick Dwyer (coderpatros) · #92 · 12/02/20

[Re: CycloneDX Node.js Module v2.0.0 Now Available](#)

Not entirely. CycloneDX v1.2 will be fully supported in DT 4.0.
By Steve Springett · #91 · 08/10/20

[Re: CycloneDX Node.js Module v2.0.0 Now Available](#)