Evolving vulnerabilities in CycloneDX

Gareth Rushgrove

snyk

Gareth Rushgrove

VP Products, Snyk

Devops Weekly curator

Conftest/Open Policy Agent maintainer

Open Source contributor

@garethr

snyk

Agenda

01 CycloneDX introduction

02 Vulnerability extension improvements

03 Next steps

snyk

CycloneDX

Very quick introduction

snyk

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">e8f33e424f3f4ed6db76a482fde1a5298970e442c531729119e37991884bdffab4f9426b7ee11fccd07
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": "e6b1000b94e835ffd37f4c6dcbdad43f4b48a02a"
        },
        {
          "alg": "SHA-256",
          "content": "f498a8ff2dd007e29c2074f5e4b01a9a01775c3ff3aeaf6906ea503bc5791b7b"
        },
        {
          "alg": "SHA-512",
```

Evolving vulnerabilities

Data modelling and suggested improvements

snyk

Vulnerability extension

Adds `.vulnerabilities` property to CycloneDX SBOM

182 lines (182 sloc) | 6.23 KB

Raw Blame

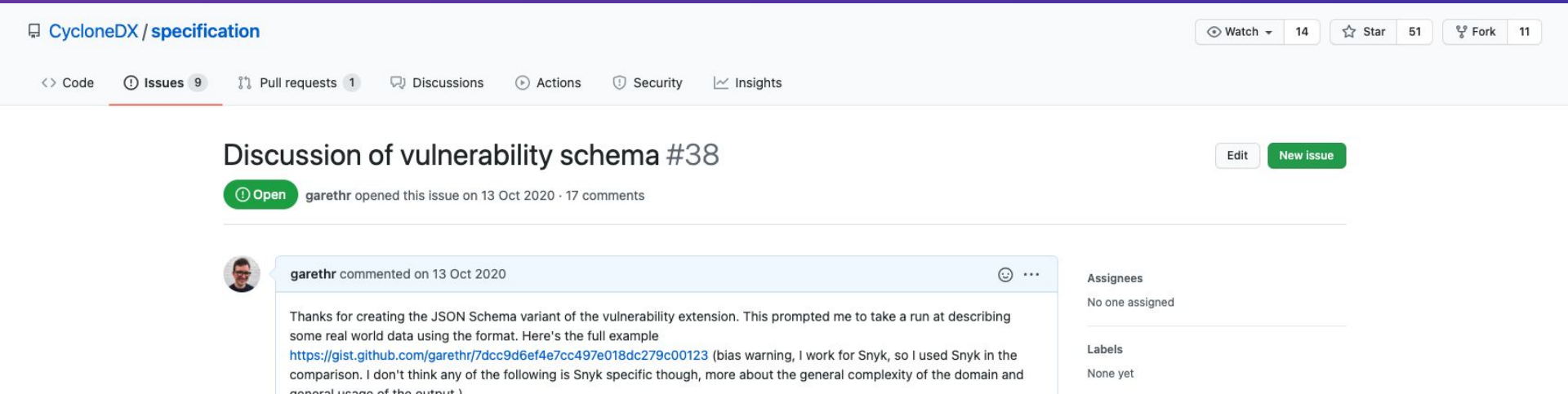
```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "$id": "http://cyclonedx.org/schema/ext/vulnerability-1.0-SNAPSHOT.schema.json",
  "type": "object",
  "title": "CycloneDX Vulnerability Extension",
  "$comment" : "CycloneDX Vulnerability Extension for JSON Schema is published under the terms of the Apache License 2.0.",
  "properties": {
    "vulnerabilities": {
      "$id": "#/properties/vulnerabilities",
      "type": "array",
      "items": {"$ref": "#/definitions/vulnerability"},
      "title": "Vulnerabilities",
      "description": "Defines a list of vulnerabilities."
    }
  },
  "definitions": {
    "cwe": {
      "type": "integer",
```

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



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/DATE10RSA.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"}
]
```

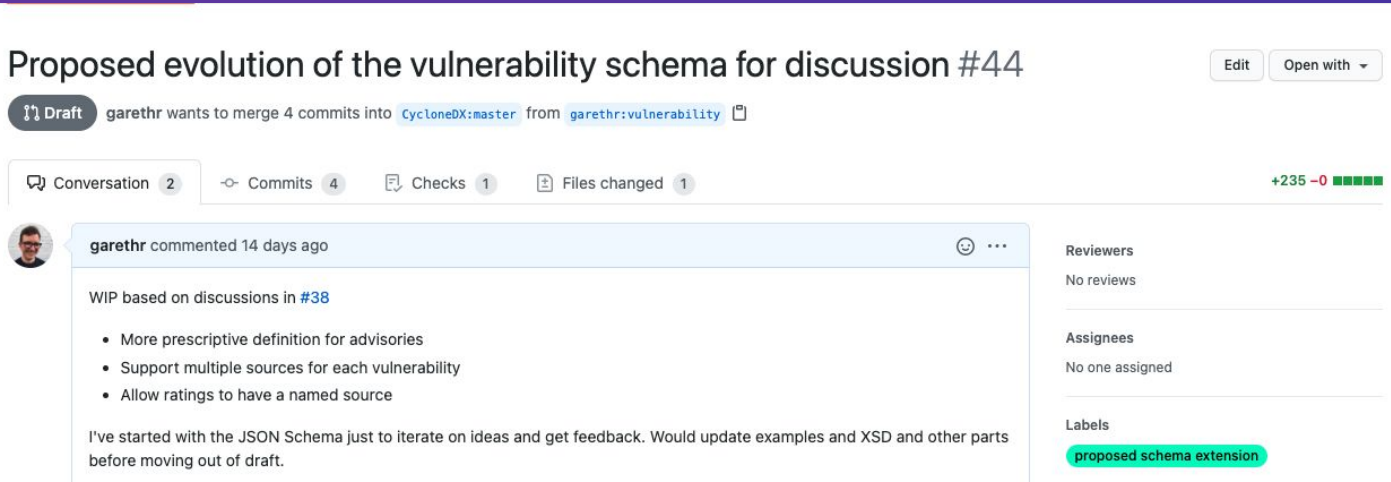
Conclusion

Next steps and getting involved

snyk

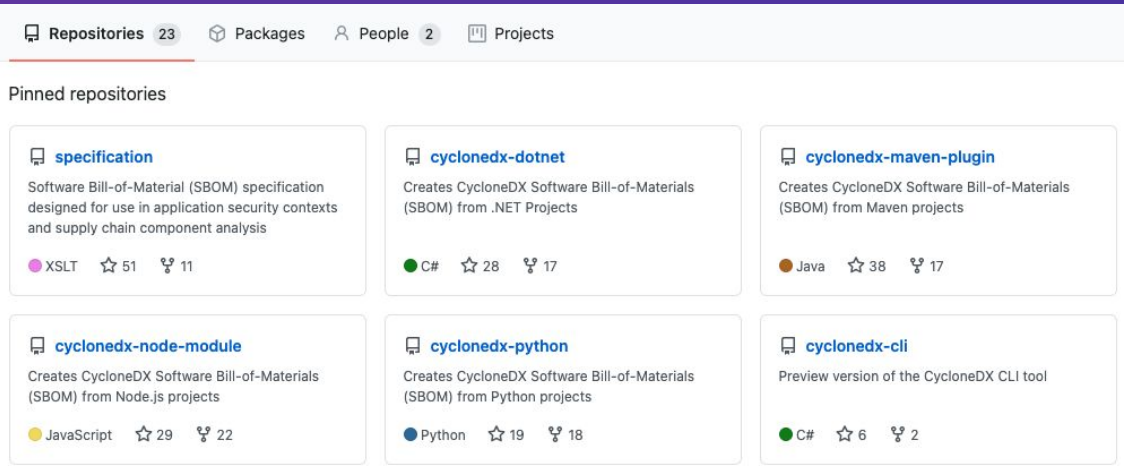
Feedback

I'd love feedback on the open PR



Experiment

Lots of tools to try out and contribute to



Discuss

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