Remediation and Disclosure

NTIA VEX Subgroup

21 October 2020

CycloneDX

The CycloneDX Approach

- Easy to adopt – easy to contribute
- Identify risk to as many adopters as possible, as quickly as possible
- Avoid any/all blockers that prevent the identification of risk
- Continuous improvement – Innovate quickly, improve over time
- Encourage innovation and competition through extensions
- Produce immutabe and backward compatible releases
- Facts first – Dynamic facts and observations enabled through extensions
- Automation and optimization of BOM creation
- Full-stack BOM specification

CycloneDX Core

- The main (default) schema
- Supports static factual information

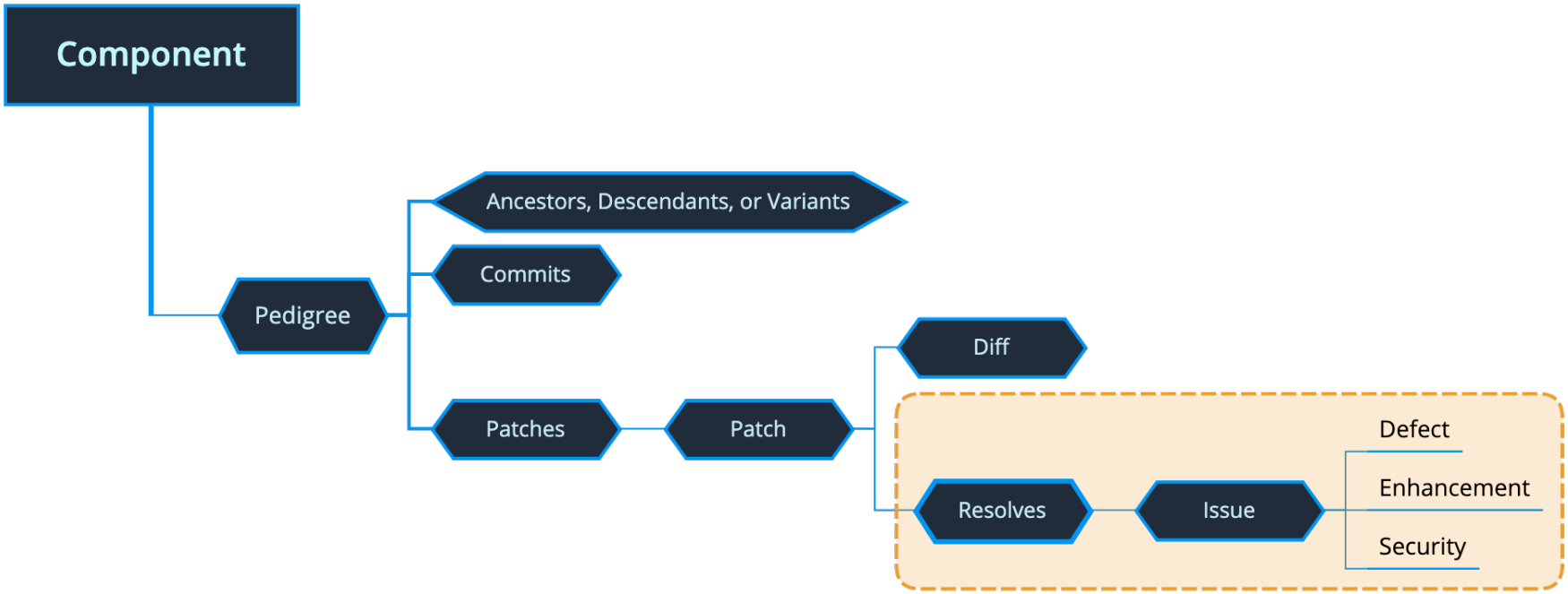
CycloneDX Extensions

- Provides optional capabilities on top of the core
- Supports opinions, observations, and dynamic factual information

Remediation and Disclosure

- CycloneDX natively supports remediation
  - Static facts – does not change
- CycloneDX supports disclosing component vulnerabilities
  - Dynamic facts - available through an extension

Component Remediation



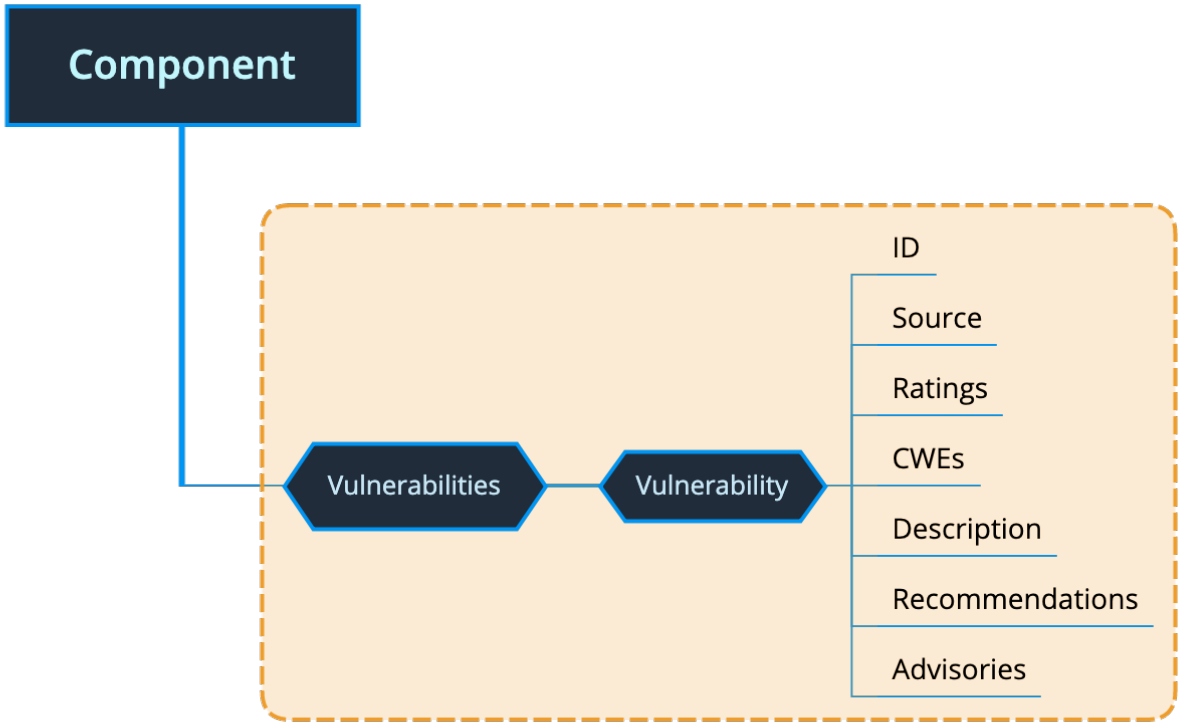
Component Remediation

```xml
<patch type="backport">
    <diff>
        <text content-type="text/plain" encoding="base64">ZXhhbXBsZSBkaWZmIGhlcmU=</text>
        <url>uri/to/changes.diff</url>
    </diff>
    <resolves>
        <issue type="security">
            <id>CVE-2019-9997</id>
            <name>CVE-2019-9997</name>
            <description>Issue description here</description>
            <source>
                <name>NVD</name>
                <url>https://nvd.nist.gov/vuln/detail/CVE-2019-9997</url>
            </source>
            <references>
                <url>http://some/other/site-1</url>
                <url>http://some/other/site-2</url>
            </references>
        </issue>
    </resolves>
</patch>
```

Remediation Notes

- CycloneDX does not attempt to communicate remediation effectiveness
  - Out of scope for core (expert opinion)
- CycloneDX does not describe build, runtime, or environmental remediation
  - Out of scope for spec
  - Possible to describe in configuration management tools

Vulnerability Disclosure



Vulnerability Disclosure

```xml
<v:vulnerability ref="pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.9.9">
    <v:id>CVE-2018-7489</v:id>
    <v:source name="NVD">
        <v:url>https://nvd.nist.gov/vuln/detail/CVE-2018-7489</v:url>
    </v:source>
    <v:ratings>
        <v:rating>
            <v:score>
                <v:base>9.8</v:base>
                <v:impact>5.9</v:impact>
                <v:exploitability>3.0</v:exploitability>
            </v:score>
            <v:severity>Critical</v:severity>
            <v:method>CVSSv3</v:method>
            <v:vector>AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</v:vector>
        </v:rating>
    </v:ratings>
    <v:cwes>
        <v:cwe>184</v:cwe>
        <v:cwe>502</v:cwe>
    </v:cwes>
    <v:description>Description Here</v:description>
    <v:recommendations>
        <v:recommendation>Upgrade</v:recommendation>
    </v:recommendations>
    <v:advisories>
        <v:advisory>https://github.com/FasterXML/jackson-databind/issues/1931</v:advisory>
    </v:advisories>
</v:vulnerability>
```

Disclosure Notes

- Vulnerability extension communicates instances of vulnerabilities
  - Vulnerability can only apply to a single component
  - Possible to risk rate each instance independently
  - May increase BOM size – unable to reuse vulnerabilities
- Miscellaneous design improvements
  - Working with Snyk
  - https://github.com/CycloneDX/specification/issues/38