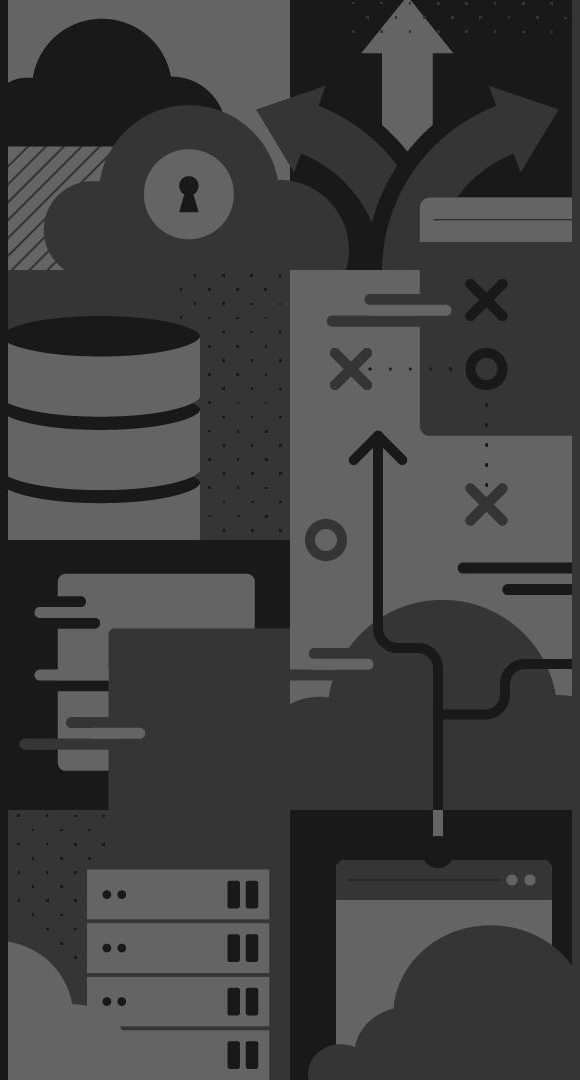


CSAF/VEX: Improved Security Data

VulnCon 2024

Martin Prpič - mprpic@redhat.com

Red Hat

`pkg:generic/redhat/mprpic@1.36.0?arch=human`

- 14 years at Red Hat
- 10 years in Red Hat Product Security
- Member of CVE AWG, CSAF TC, OpenEoX TC

Evolution of publishing machine-readable security data

- Level 0: no data at all

Evolution of publishing machine-readable security data

- Level 0: no data at all
- **Level 1: free-form text**

Evolution of publishing machine-readable security data

- Level 0: no data at all
- Level 1: free-form text
- **Level 2: custom, machine-readable format**

Evolution of publishing machine-readable security data

- Level 0: no data at all
- Level 1: free-form text
- Level 2: custom, machine-readable format
- **Level 3: industry standard for machine-readable vulnerability metadata**

Evolution of publishing machine-readable security data

- Level 0: no data at all
- Level 1: free-form text
- Level 2: custom, machine-readable format
- Level 3: industry standard for machine-readable vulnerability metadata
- **Level 4: AI patches all vulnerabilities ¯_(ツ)_/¯**

Vulnerability Exploitability eXchange (VEX)

- Used to "assert the status of specific vulnerabilities in a particular product"
- Example:
  - **libfoo in versions 2.0.0 to 2.5.6 are vulnerable to CVE-2038-0119; version 2.5.7 fixes this vulnerability; versions 1.0.0 to 1.1.7 are not affected**
    - Versions must be comparable
    - Ranges (or range bounds) must be explicitly specified
    - Affectedness status must be standardized
    - Component and vulnerability must be identified

CSAF VEX

- **VEX is a profile in the Common Security Advisory Format (CSAF 2.0) that defines required fields and values to provide vulnerability affectedness statements**
- Notable features:
  - Identifying products by CPEs (among other product identifiers)
  - Allows correlation of components to products via tree-based definitions
  - Components by PURL
  - Vulnerabilities by CVE IDs
  - Linking to SBOMs

Red Hat's VEX implementation

- Single CSAF file per product version released through a security advisory:
  - `advisories/2022/rhsa-2022_7777.json`
- Single CSAF file per published vulnerability (identified by a CVE):
  - `vex/2023/cve-2023-1111.json`

Motivation:

- Red Hat has a large variety of products, some with 1000s of components
- A single vulnerability may affect a large number of products/components
- Example: RHEL vs Ansible vs OpenShift

Product composition

- Product and component definitions are defined in a `product_tree` element, and contain references to CPEs and purls that are consistent across the entire security data set


```
"product_tree": {
  "branches": [
    {
      "branches": [
        {
          "branches": [
            {
              "category": "product_name",
              "name": "Red Hat Build of Quarkus",
              "product": {
                "name": "Red Hat Build of Quarkus 2.13",
                "product_id": "8Base-RHBQ-2.13",
                "product_identification_helper": {
                  "cpe": "cpe:/a:redhat:quarkus:2.13::el8"
                }
              }
            }
          ],
          "category": "product_family",
          "name": "Red Hat build of Quarkus (RHBQ)"
        },
        {
          "branches": [
            {
              "category": "product_version",
              "name": "apache-mime4j-core",
              "product": {
                "name": "apache-mime4j-core:0.8.3.redhat-00008",
                "product_id": "apache-mime4j-core:0.8.3.redhat-00008",
                "product_identification_helper": {
                  "purl": "pkg:maven/redhat/apache-mime4j-core@0.8.3.redhat-00008?type=jar"
                }
              }
            }
          ]
        }
      ],
      "category": "vendor",
      "name": "Red Hat"
    }
  ]
}
```


Red Hat

Product-to-component relationships

```
"relationships": [
  {
    "category": "default_component_of",
    "full_product_name": {
      "name": "apache-mime4j-core:0.8.3.redhat-00008 as a component of Red Hat build of Quarkus (RHBQ)",
      "product_id": "8Base-RHBQ-2.13:apache-mime4j-core:0.8.3.redhat-00008"
    },
    "product_reference": "apache-mime4j-core:0.8.3.redhat-00008",
    "relates_to_product_reference": "8Base-RHBQ-2.13"
  }
]
```

- Relationships between products and components provide the ability to assert the affectedness of both

Vulnerability

- One object identified by a single CVE ID along with its metadata:
  - Textual descriptions
  - Mitigation statements
  - CVSS ratings
  - Impact
  - External references
  - ...


```
"vulnerabilities": [
  {
    "cve": "CVE-2022-45787",
    "cwe": {
      "id": "CWE-787",
      "name": "Out-of-bounds Write"
    },
    "discovery_date": "2023-01-06T00:00:00Z",
    "ids": [
      {
        "system_name": "Red Hat Bugzilla",
        "text": "https://bugzilla.redhat.com/show_bug.cgi?id=2158916"
      }
    ],
    "notes": [
      {
        "category": "description",
        "text": "A flaw was found in Apache James's Mime4j ...
        "title": "Vulnerability description"
      },
      {
        "category": "summary",
        "text": "Temporary File Information Disclosure in...",
        "title": "Vulnerability summary"
      }
    ],
    ...
```

Vulnerability product statuses

```
"product_status": {
  "known_affected": [
    "8Base-RHBQ-2.13:apache-mime4j-core:0.8.3.redhat-00008"
  ]
},
"remediations": [
  {
    "category": "none_available",
    "details": "The fix for this vulnerability is not yet available.",
    "product_ids": [
      "8Base-RHBQ-2.13:apache-mime4j-core:0.8.3.redhat-00008"
    ]
  }
]
```

first_affected
first_fixed
fixed
known_affected
known_not_affected
last_affected
recommended
under_investigation

```
"product_status": {
  "fixed": [
    "8Base-RHBQ-2.13:quarkus-vertx-http:2.13.7.Final-redhat-00003"
  ]
},
"remediations": [
  {
    "category": "vendor_fix",
    "details": "For details on how to apply this update, ..."
    "product_ids": [
      "8Base-RHBQ-2.13:quarkus-vertx-http:2.13.7.Final-redhat-00003"
    ],
  }
]
```


Red Hat

Connecting VEX and SBOM

SBOM

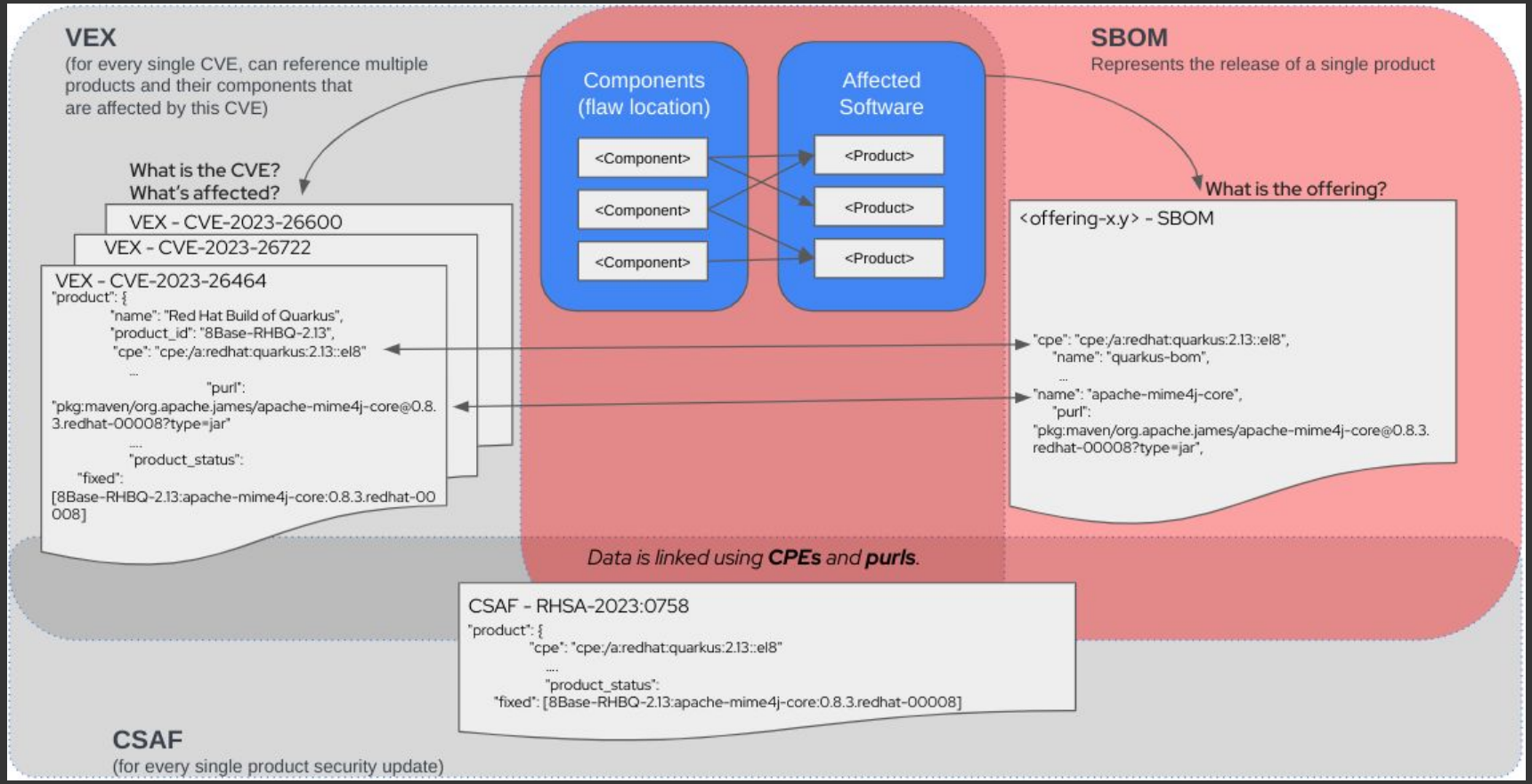
Procurement and Audit

Manifest
Provenance
Licensing

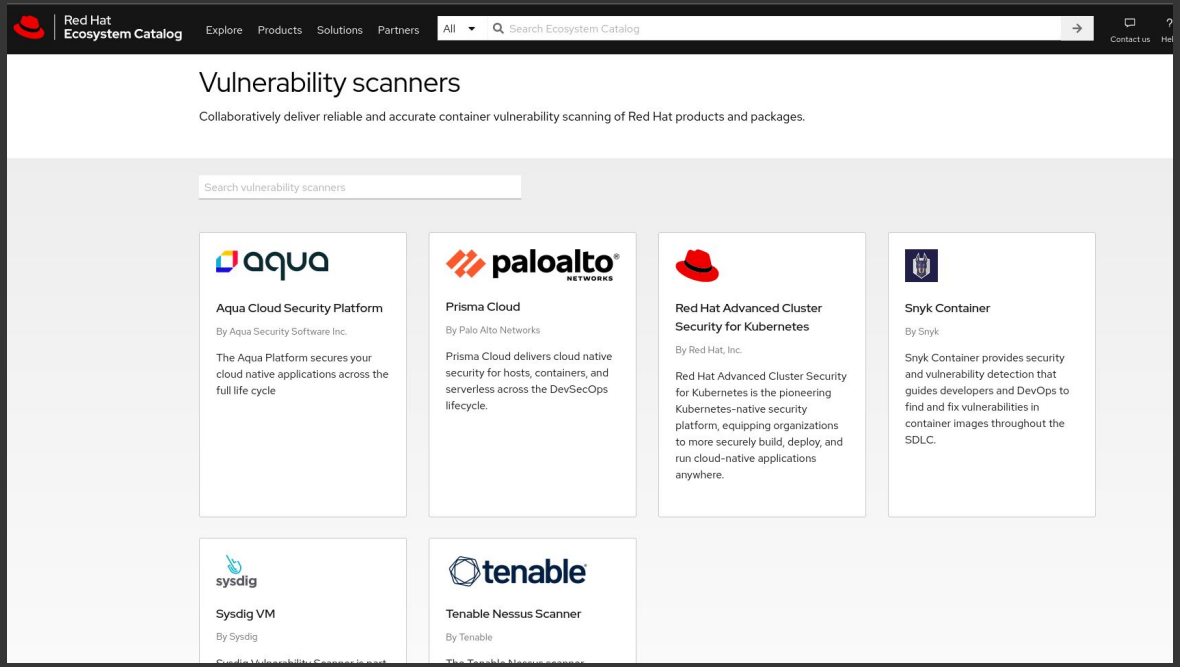
VEX

Risk Management

Vulnerability Management
Exploits
Incident Response

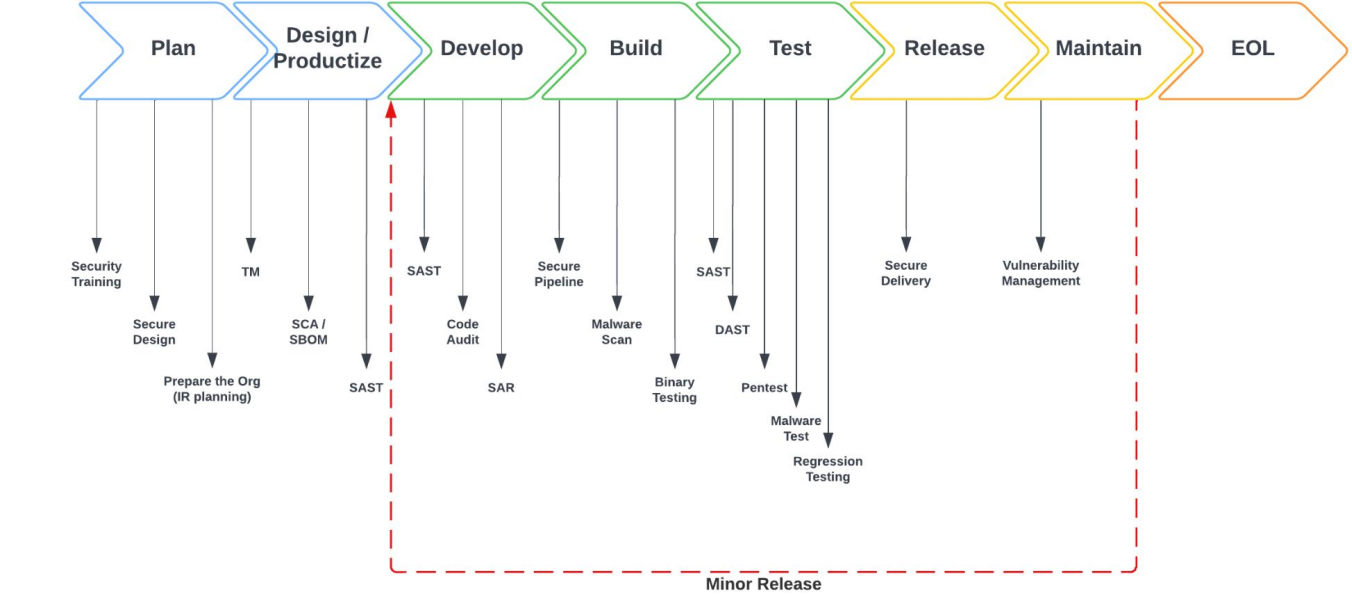

VEX
(for every single CVE, can reference multiple products and their components that are affected by this CVE)
What is the CVE?
What's affected?
VEX - CVE-2023-26600
VEX - CVE-2023-26722
VEX - CVE-2023-26464
"product": {
"name": "Red Hat Build of Quarkus",
"product_id": "8Base-RHBQ-2.13",
"cpe": "cpe:/a:redhat:quarkus:2.13::el8"
...
"purl":
"pkg:maven/org.apache.james/apache-mime4j-core@0.8.3.redhat-00008?type=jar"
....
"product_status":
"fixed":
[8Base-RHBQ-2.13:apache-mime4j-core:0.8.3.redhat-00008]
Components (flaw location)
<Component>
<Component>
<Component>
Affected Software
<Product>
<Product>
<Product>
SBOM
Represents the release of a single product
What is the offering?
<offering-x.y> - SBOM
"cpe": "cpe:/a:redhat:quarkus:2.13::el8",
"name": "quarkus-bom",
...
"name": "apache-mime4j-core",
"purl":
"pkg:maven/org.apache.james/apache-mime4j-core@0.8.3.redhat-00008?type=jar",
Data is linked using CPEs and purls.
CSAF - RHSA-2023:0758
"product": {
"cpe": "cpe:/a:redhat:quarkus:2.13::el8"
....
"product_status":
"fixed": [8Base-RHBQ-2.13:apache-mime4j-core:0.8.3.redhat-00008]
CSAF
(for every single product security update)

Red Hat Vulnerability Scanner Exchange



Red Hat

Producing VEX as part of Secure Development Lifecycle



Red Hat

Producing VEX as part of Secure Development Lifecycle

- A VEX statement represents the end result of two actions:
  - **Initial analysis of the vulnerability's affectedness to a product/component**
    - Analysis should be done based on data from existing SBOMs
    - Part of the *Maintain* SDL phase

Producing VEX as part of Secure Development Lifecycle

- A VEX statement represents the end result of two actions:
  - Initial analysis of the vulnerability's affectedness to a product/component
    - Analysis should be done based on data from existing SBOMs
    - Part of the *Maintain* SDL phase
  - **A publication of a fix for an affected product/component**
    - A security advisory is published that asserts that a fix was made to a new version of a product/component; VEX statement is updated
    - SBOM for the new product is published with new versions matching those noted in the security advisory
    - Part of the *Release* SDL phase

Mapping vulnerability metadata to product support models

- **Assertions of affectedness must be aware of product versions**
  - Example: a vulnerability fixed in Red Hat OpenShift 4.15 (latest version) is assumed to be fixed in all future releases
  - Example: a vulnerability fixed in Red Hat OpenShift 4.15 is applicable only to that one product version, while OpenShift 4.13 or 4.14 (supported versions) are still considered as affected

Mapping vulnerability metadata to product support models

- **Machine-readable product support life cycle**
  - https://openeox.org/

Challenges & Improvements

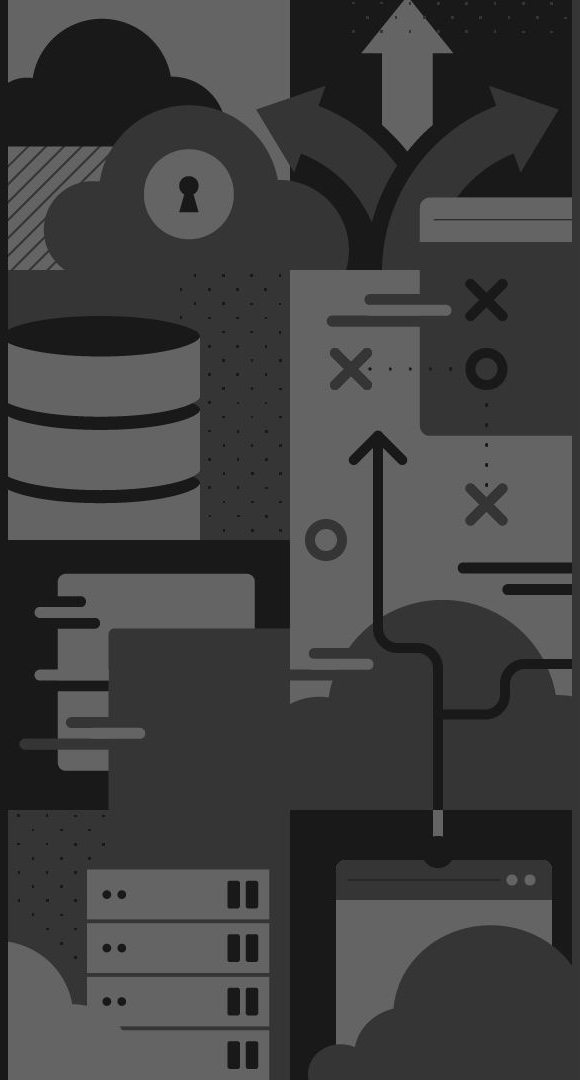
- Enforcing consistent vulnerability remediation data capture at organizational level

Challenges & Improvements

- Enforcing consistent vulnerability remediation data capture at organizational level
- **Ambiguity in security data standards**
  - `pkg:rpm/rhel/audit-libs@3.0.7-5.el8?arch=x86_64&distro=rhel-8.9`
  - `pkg:rpm/redhat/audit-libs@3.0.7-5.el8?arch=x86_64distro=rhel-8`

Challenges & Improvements

- Enforcing consistent vulnerability remediation data capture at organizational level
- Ambiguity in security data standards
  - `pkg:rpm/rhel/audit-libs@3.0.7-5.el8?arch=x86_64&distro=rhel-8.9`
  - `pkg:rpm/redhat/audit-libs@3.0.7-5.el8?arch=x86_64distro=rhel-8`
- **Expressing assumed affectedness**
  - CVE-1234-5678 affects the Windows kernel, do I need to publish a VEX statement asserting that the Linux kernel is not affected?



Q&A

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Red Hat