CRAVEX: Managing-Vulnerabilities-in-DejaCode

This design is ready for review.

CRAVEX project: See https://github.com/orgs/aboutcode-org/projects/8/views/1

Background

Objective: Use Vulnerability Risk, Weighted Severity and Exploitability values from VulnerableCode to manage vulnerabilities in DejaCode.

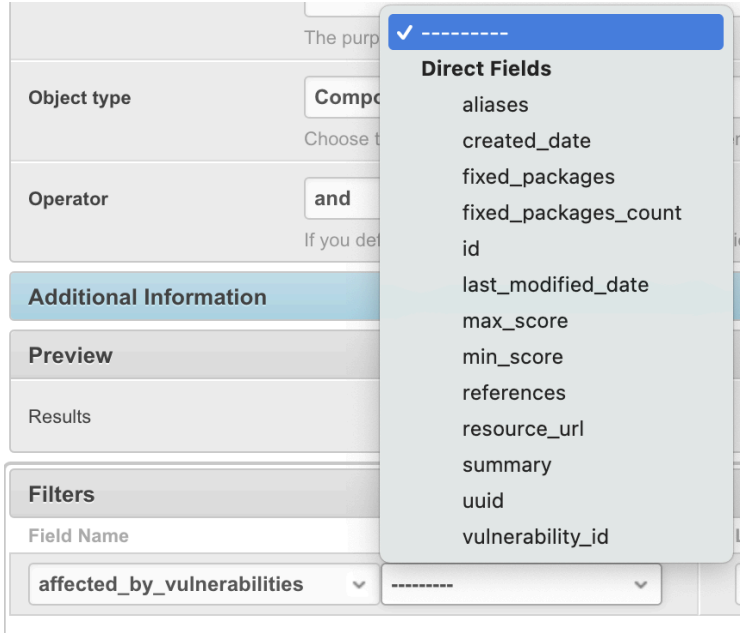
Related GitHub issues:

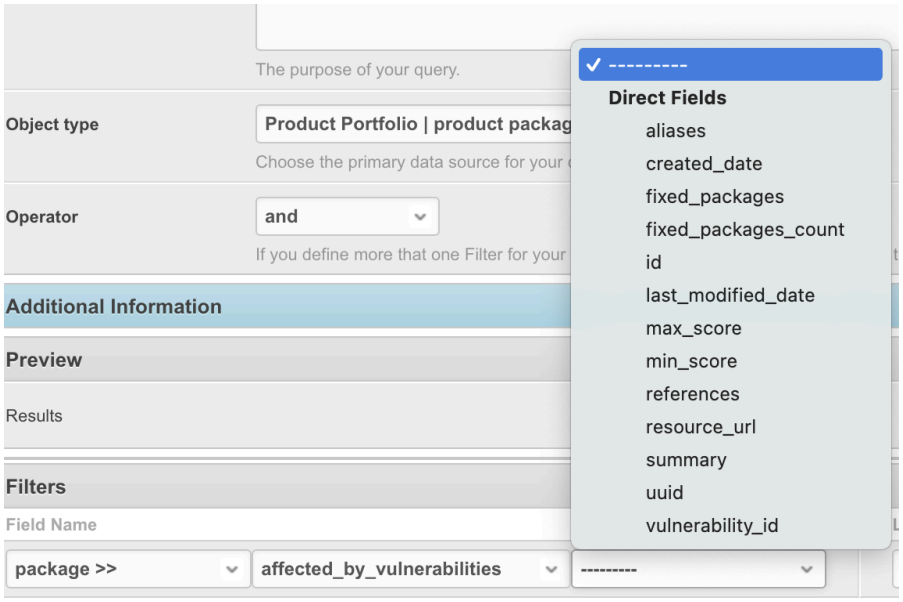
- https://github.com/aboutcode-org/dejacode/issues/97

- https://github.com/aboutcode-org/dejacode/issues/15
- https://github.com/aboutcode-org/dejacode/issues/98

Update DejaCode Packages with Vulnerability Scores

DejaCode has a process that updates Packages with VulnerableCode data on a routine scheduled basis (such as daily). This makes vulnerability data fields available to the DejaCode user in Package and Product Package Queries.





Rather than **max_score** and **min_score**, DejaCode should be improved to get three new score values supported by https://github.com/aboutcode-org/vulnerablecode/issues/1543 and https://github.com/aboutcode-org/dejacode/issues/97 :

- **Weighted Severity**. A number ranging from 0 to 10 calculated from the severity scores provided by various data sources and the weight values assigned to each data source depending on its reliability and authority.

- **Exploitability**. A number ranging from 0.5 to 2 that refers to the **potential or probability** of a software package vulnerability being exploited by malicious actors to compromise systems, applications, or networks, andis determined automatically by discovery of exploits.

- **Vulnerability Risk**. A number ranging from 0 to 10 calculated from weighted severity and exploitability values.

These scores support the DejaCode user's ability to prioritize review and determine action when reviewing Packages and Product Packages.

DejaCode should also set the Vulnerability Status (see next section) to "Under Investigation" when a Vulnerability is initially discovered for a Package.

Vulnerability Status

introduce a "**Vulnerability Status**" table to define status codes that can be applied to Package and Product Package. (We need one anyway to support VEX.) Reference Data Values (fixture values) should be

- None Identified (the default)

and the standard VEX Status values as defined for the "state" field in the CDX VEX spec:
https://cyclonedx.org/docs/1.6/json/#vulnerabilities_items_analysis

- "resolved"
- "resolved_with_pedigree"
- "exploitable"
- "in_triage" applied automatically to a Package when a new vulnerability is identified for it.
- "false_positive"

Add the Vulnerability Status field to the Package and Product Package models.

DejaCode Product Package Relationship

Introduce Vulnerability Status to the Product Package Relationship. Note that it refers to the Vulnerability Status within the context of the Relationship.

When a new Product Package is created in DejaCode, set the Vulnerability Status to be the same as the one identified in the corresponding Package.

DejaCode Packages UI

The Vulnerabilities tab of the Packages detail user view in DejaCode currently is a grid with the following columns: Affected by, Aliases, Score, Summary, Fixed Packages.

This should be improved to replace the **Score** column (which currently shows a Severity range) with three new columns that provide the **Weighted Severity, Exploitability, and Vulnerability Risk** score values. Enable sorting and filtering on those columns.

DejaCode Product UI

Product Inventory Tab

The Product Inventory tab in DejaCode currently is a grid with the following columns: Item, Purpose, Concluded license, Review status, Deployed, Modified.

This should be improved to:

- Modify the layout of the Item label cell to move the “Is vulnerable” dropdown button to the left so that it is just to the right of the “Show/Hide details” dropdown button. (Note that the current position of this button strongly implies that the little usage policy icon in each Item refers to vulnerability status rather than license compliance usage policy for the Item.)
- Replace the label of “Review status” with “**Compliance status**”
- Just after the “Compliance status” column, introduce a new “**Vulnerability status**” column and enable filtering on it.

Apply the label name change, and introduce the new “Vulnerability status” field, in the “Update relationship” form.

Product Vulnerabilities Tab

The Product Vulnerabilities tab in DejaCode currently is a grid with the following columns: Vulnerability, Aliases, Score, Summary, Affected packages.

This should be improved to replace the **Score** column (which currently shows a Severity range) with three new columns that provide the **Weighted Severity, Exploitability, and Vulnerability Risk** score values. Enable sorting and filtering on those columns.

The Vulnerabilities tab on Product could possibly highlight specific items based on their Risk value:

8.0 - 10.0 Critical, immediate response required (red?)

6.0 - 7.9 High, response required as soon as possible (orange?)

3.0 - 5.9 Medium, investigation required (yellow?)

0.1 - 2.9 Low, response deferred (no highlight)

Also we can use the ranges defined above for filtering by Risk.

Additional Notes and Discussion

-