Risk Acceptance

This document intends to provide some information about the process to Risk Accept a vulnerabilities and possible workflows that could be followed to achieve a better result.

There will be a section where we are going to talk about Custom Fields, how to create them and for what reason.

We will provide as much information as possible in this document, and if you would like to discuss this on a meeting, please let us know.

Information provided by the Customer:

The customer would like to start Risk Accepting vulnerabilities in the Kenna platform.

There are some vulnerabilities that should have been marked as Risk Accepted but were not, and due to that, the Total Risk Score is still using those vulns to calculate its value and impacting some of their analysis.

NOTE from Kenna: Even when changing a vulnerability status to "Risk Accepted," the Total Risk Score and the Risk Meter score might not change at all, and here is way:

The overall Risk Meter score is an average of all the NON-Zero score Assets included in that group. Example:

Asset Name	Score
ALB01	1000
ALB02	1000
ALB03	0
ONT01	580
ONT02	950

Calculation:	(	ALB01	+	ALB02	+	ONT01	+	ONT02	)	/	4	=	Risk Meter score
		1000		1000		580		950					880

Each Asset's Risk Score in Kenna is based on the single greatest vulnerability found on the asset. While each individual asset in the Asset Group will have any number of vulnerabilities associated with it, the asset score, is only based on the highest vulnerability.

Due to that, even if you are Risk Accepting some critical vulnerabilities (score 100) under a specific asset, but there are still other critical vulns there (score 100), the asset will not change its score and because of that the Risk Meter score will not change as well.

We do not recommend using the Risk Accepted process to only decrease the Risk Score. The change of status in the vulnerability needs to be planned and evaluated so you do not miss critical vulnerabilities that needs to be patched/fixed and were not.

Information from the Kenna CSE Team:

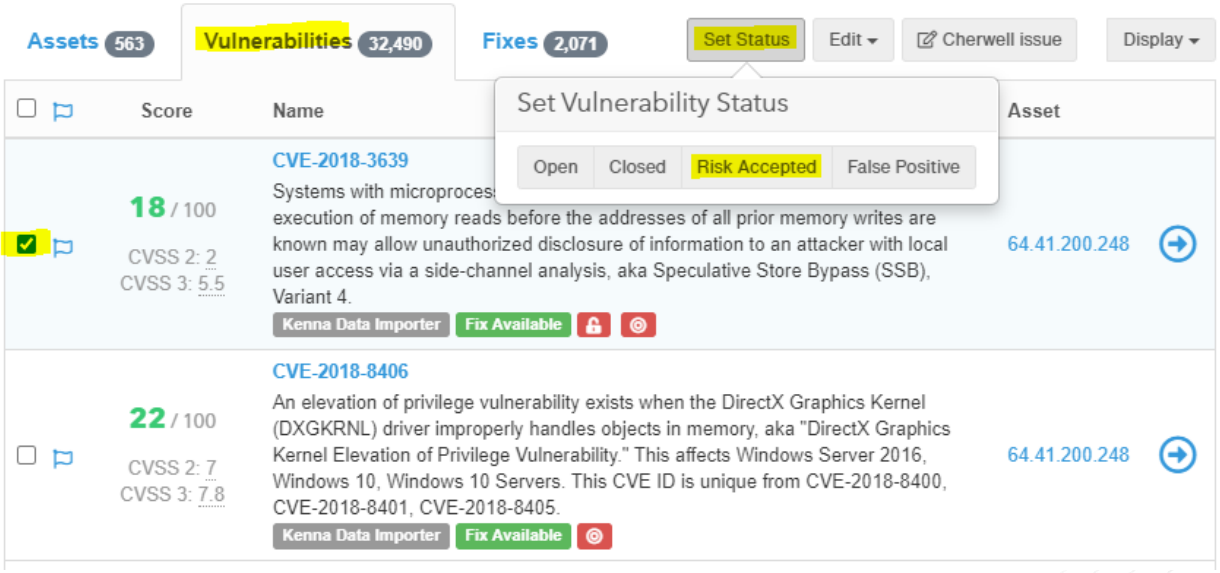
In Kenna, all vulnerabilities have 4 possible statuses: Open, Closed, Risk Accepted, & False Positive, and there are a few places from where you can change the vulnerability status.

Before diving into on how to change the vulnerability status, we would like to share some important information:

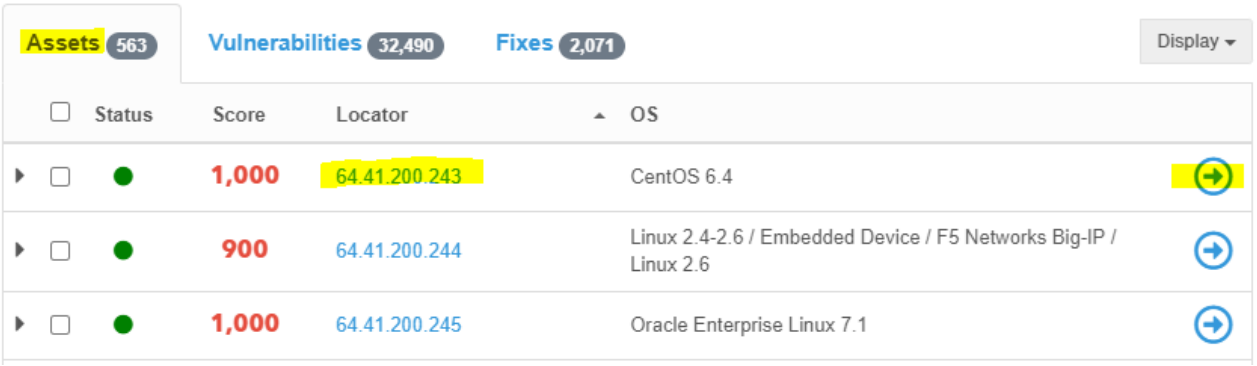
> **Risk Accepted:** The vulnerability truly represents a risk, but the business has decided not to remediate it for some reason. A good example of a Risk Accepted vulnerability is an Internet Explorer vulnerability on a server in a data center that is not accessed or Java vulnerabilities that cannot be remediated because a legacy application will not be replaced until the next fiscal year.
>
> Flagging a vulnerability as **risk accepted** will remove those items from the risk meter score, as only open vulnerabilities contribute to an asset score.

Now, lets dive into how to change the vulnerability status:

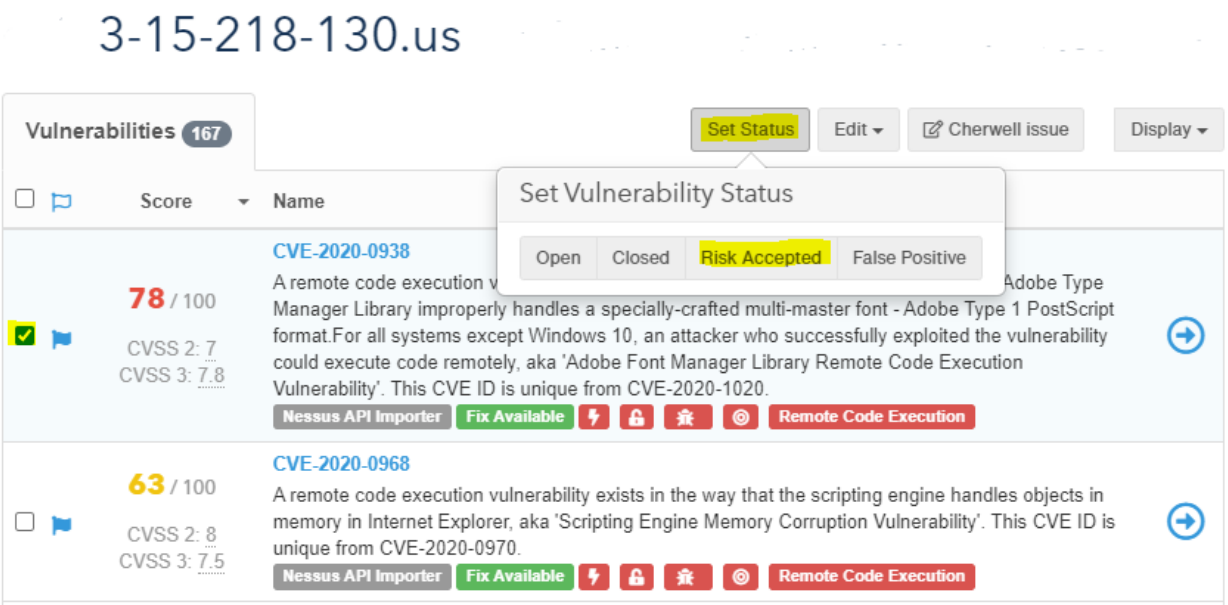
- Directly from the Explore page, under the vulnerabilities' tab:
    - You need to select the vulnerabilities that you and to change its status, and then click on "set status"



- Directly from the asset's page:
  - From the Explore page, you can either click on the asset's name or in the blue arrow at the right side of the asset's information:



  - When the new page opens, you will see all the vulnerabilities linked to that asset, and from there you can select one or more vulnerabilities and change its status:



- Directly from the Vulnerabilities' page:
    - You can access the vulnerabilities' page from either the explore page or from the asset's page:

Figure 1-Asset's Page

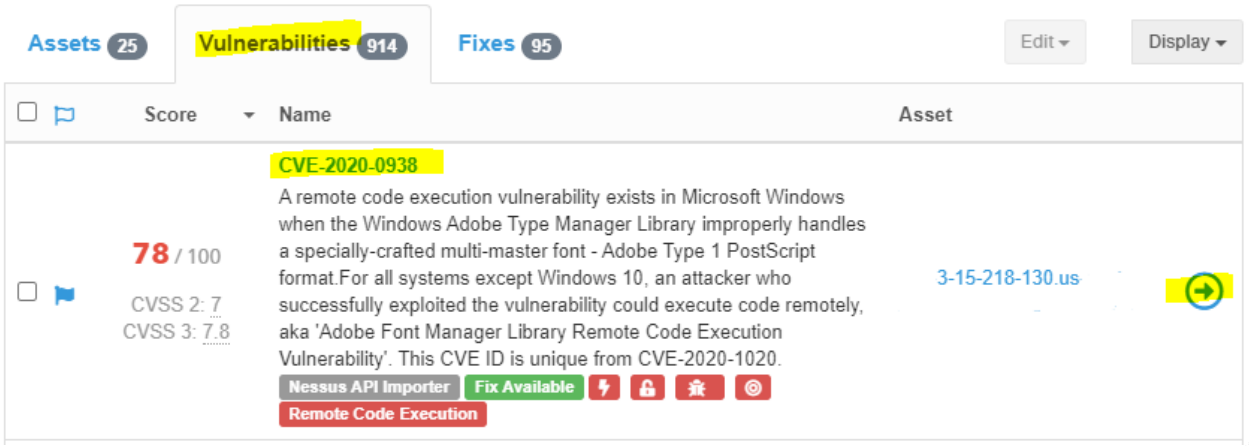
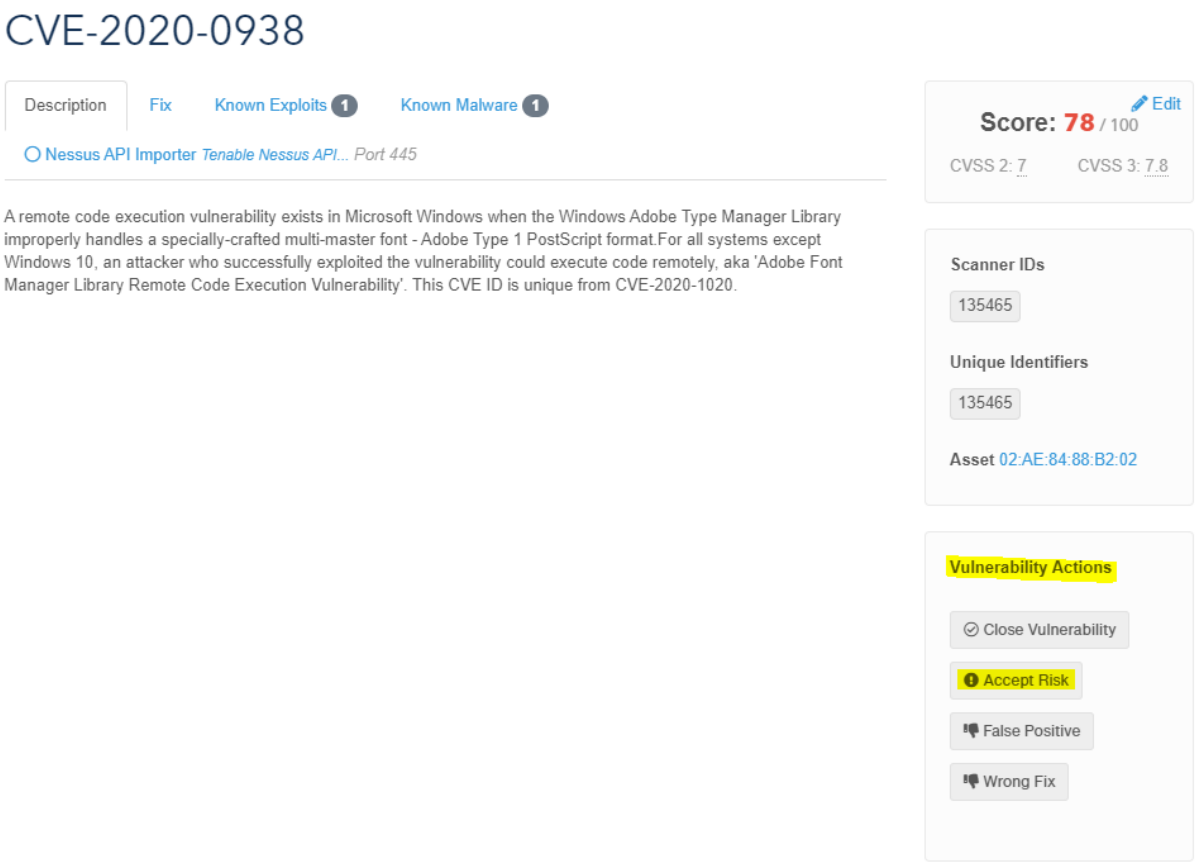


Figure 2 - Explore Page

- When the new page opens (the vulnerability page), check the right side of the page for a field called "Vulnerability Actions"



When the vulnerability status is manually changed, Kenna will not reopen that vulnerability automatically, even if the vuln information is coming from the connector run as "open." In case you need to reopen the vulnerability, you will need to follow the above steps, and select the "Open" / "Reopen Vulnerability" option.

The above steps were to show how you can change the vuln status through the UI.

There is still another option that you can use, and that is through the API (this document will not go into that process):

- Update Vulnerability
- Bulk Update Vulnerabilities

On our GitHub you can also find a script that does the needed vuln change, in case you would like to check:

- vulnerability_status_setter (look for "vulnerability_status_setter")

Risk Exception Workflow:

The following example is a consolidated view on how other customer are building/using the Risk Accepted feature in Kenna, and also some information from us:

Develop 3 (or 4) custom fields (we are going to explain how to create it in the next topic):

- Risk Acceptance Requester (type: string / show as filter)
  - Used to input the Requester's name. There are normally only a couple of requesters.
  - Try to keep the same pattern when inputting names (Ex. John Martin)
- Risk Acceptance Analyst (type: string / show as filter)
  - Used to input the Analyst's name. The person that is changing that information in Kenna.
  - The Kenna audit logs should show who changed that, but it takes time to check. It's better if you have the name in a Custom Field.
- Risk Acceptance Month end/review (type: string / show as filter) and
  - This field will be used to create new Risk Meters and to track those vulnerabilities that needs to be reassessed.
  - The normal input would be something like: Sep/2021
- Risk Acceptance Notes (maybe depending on Cutsomers requirement. Do NOT show in filter list)
  - Used only if you need to add more information about the process that was used to validate why that vulnerability was marked as Risk Accepted.
  - Could be also used to add the date when the status was manually changed and why.

Workflow:

- User puts in a request for the RA to be filed.
- Analyst reviews the request and if confirmed to be okay, updates relevant details for RA requester, RA analyst, RA month end/review - and if applicable - RA notes and then the vulnerabilities are risk accepted (changes the vulnerability status).
- As Kenna does not update these vulnerabilities when they are in a risk accepted state, they will need to be manually taken back to open before they can be updated. Month end date will be used to track what RAs are due on a month-to-month basis. Possibility of having the requesters reach out before the due month so that the flag can be removed.

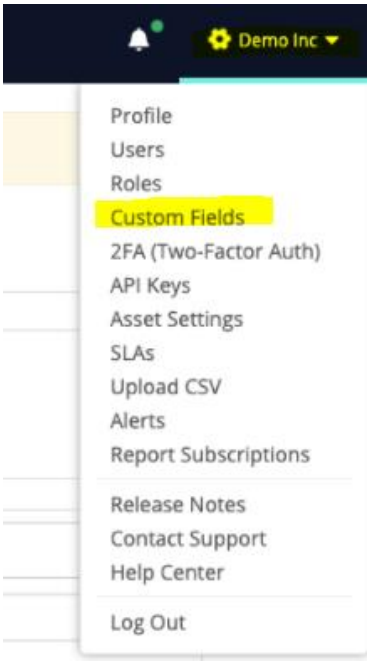
Creating Custom Field:

There are three types of custom fields:

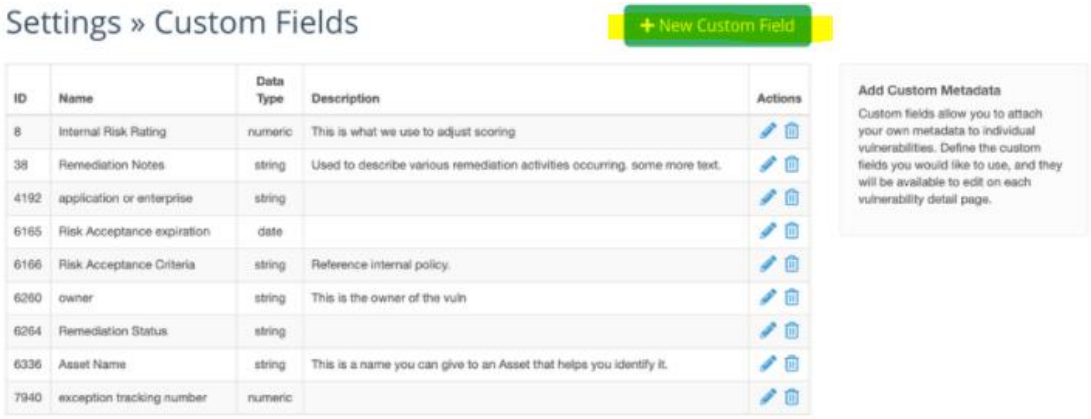
- Text Fields
    - Text fields support up to 2000 characters of text. This can be used for additional notes, marking an Owner of a vulnerability, or any other text based data.
- Date Fields
    - Date fields support a calendar date. When editing a date based custom field, a calendar popup will appear when you edit the field. You can also manually input a date in MM/DD/YYYY format. This type of custom field can be used to mark the date a vulnerability was Risk Accepted, a date to review the vulnerability status (Risk Acceptance or False Positive review/re-validation).
- Numeric Fields
    - Numeric fields support any number. This number can include decimals.

There is only one way of creating Custom Fields:

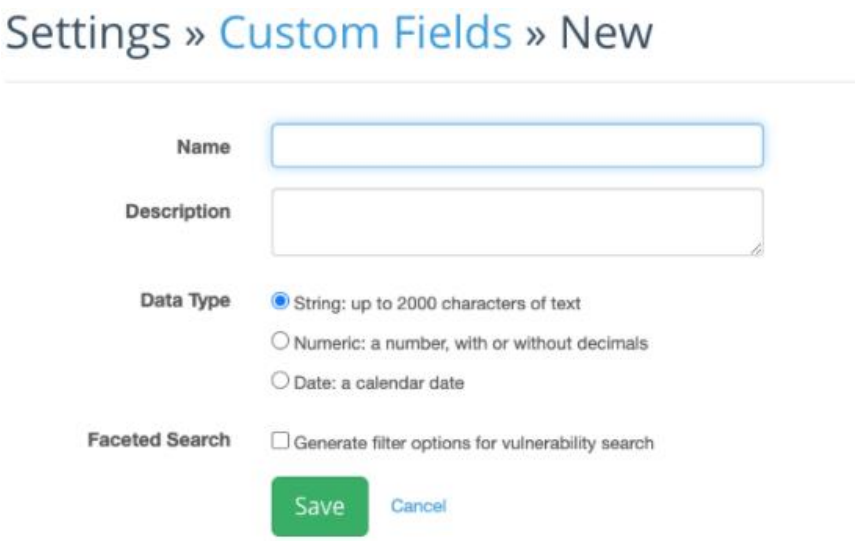
1. Navigate to the gear in the upper right-hand side of your browser when logged in and from the dropdown menu, select Custom Fields.



2. From the Custom Fields page, click + New Custom Field.



3. Complete the fields shown to include: naming the field, adding a description, selecting the type of field (Text, Date or Numeric), and filtering vulnerabilities on this field in the Explore view. If you'd like to filter on this field in Explore, simply click the checkbox for Faceted Search



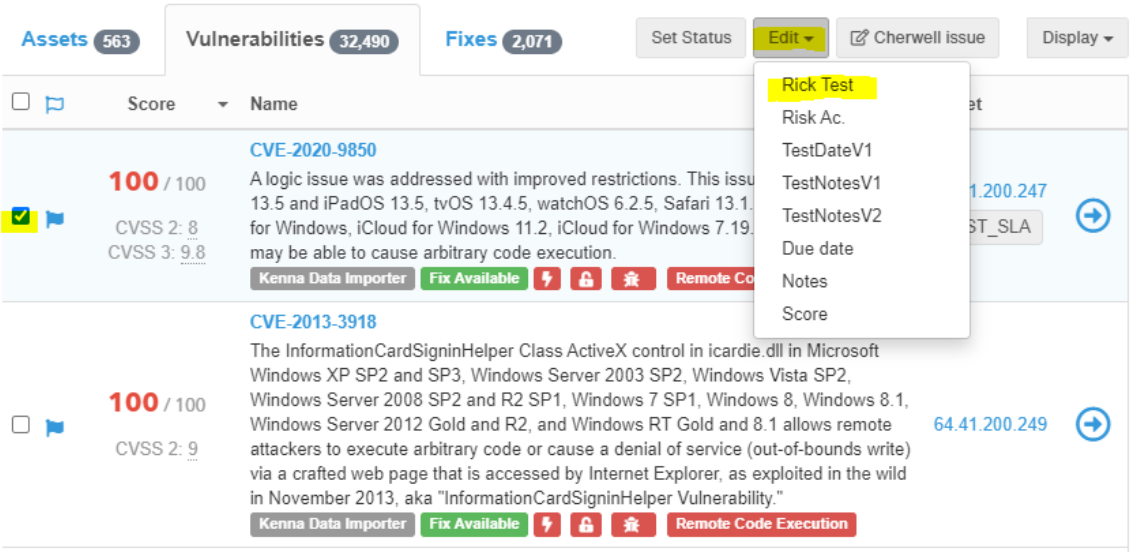
Note: For each unique entry in a custom field creates a new checkbox in Explore. For example, if you have four unique dates/numbers/text strings, it will create four checkboxes.

4. After you define your desired custom fields, they are automatically available for all vulnerabilities. You can now add data to these custom fields, individually, or in bulk if the entry you are adding is the same across a group of vulnerabilities.

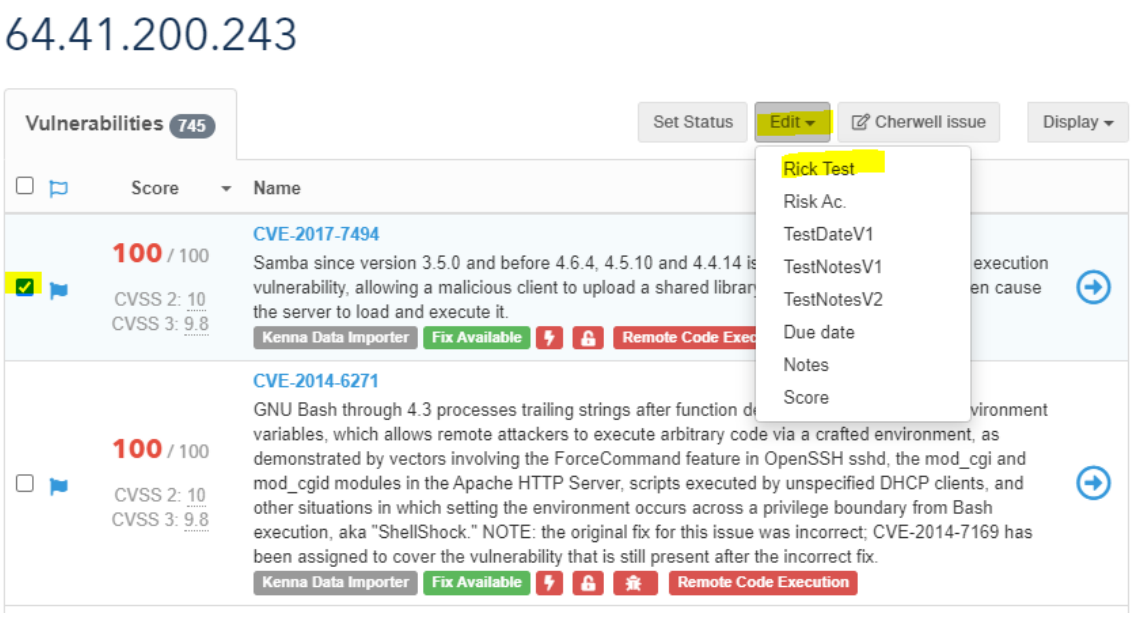
How to use the newly created Custom Fields:

There are 3 places from where you can edit the vulnerability custom fields, and they are:

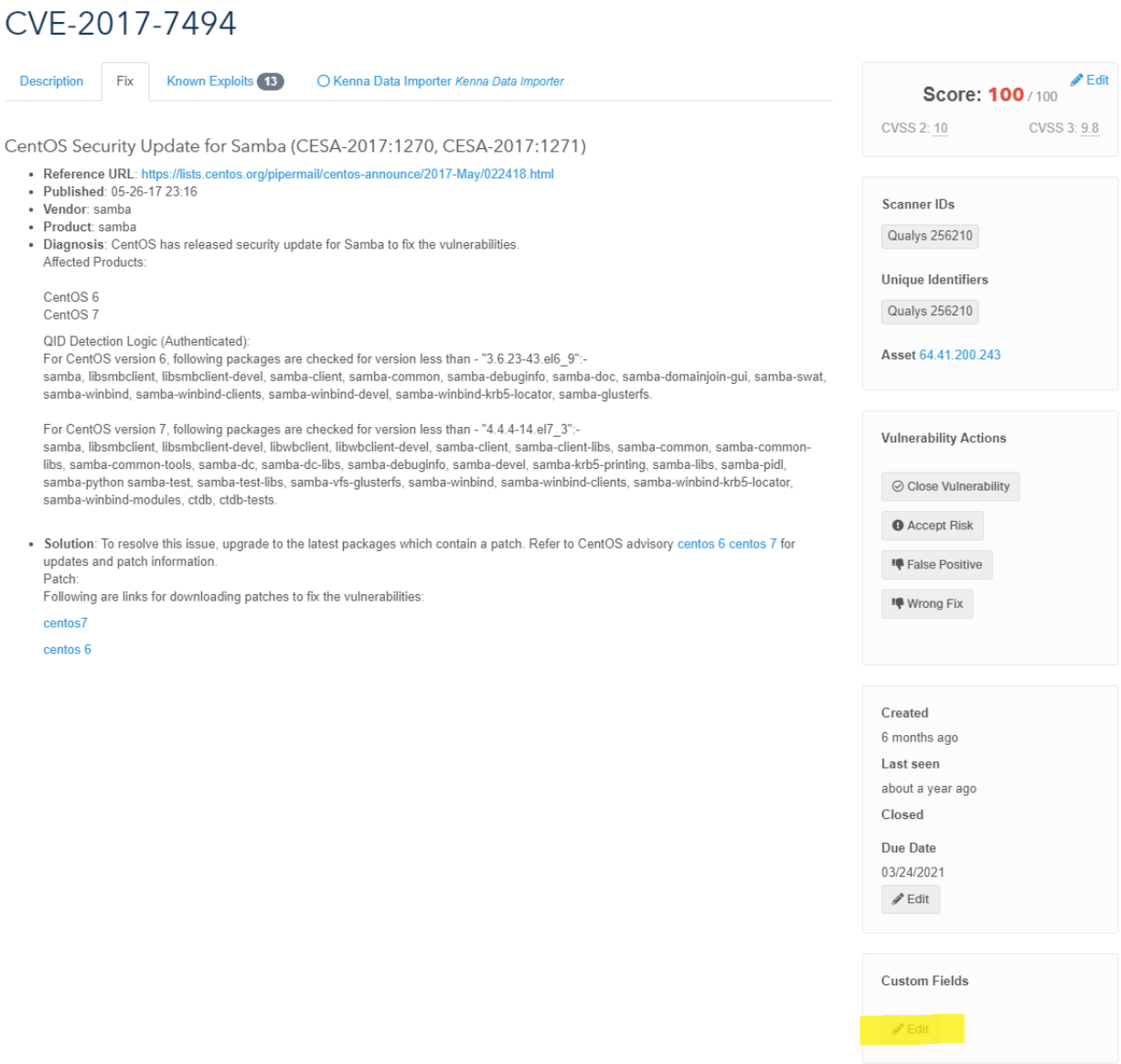
1. From the Explore's page
    a. Select the vulnerability/vulnerabilities that you want to edit.
    b. Click on the "Edit" bottom and select the Custom Field that you want to change.



2. From the Asset's page
    a. Select the vulnerability/vulnerabilities that you want to edit.
    b. Click on the "Edit" bottom and select the Custom Field that you want to change.



3. From the Vulnerability's page



How to check the True Risk Score:

When utilizing the Risk Accepted vulnerability status, Kenna's "True Risk Score" can help identify how much risk is truly present in your environment. Your "true risk score" for any given risk meter is calculated to include all risk accepted vulnerabilities that would fall into that asset group IF they were not risk accepted.

The "True Risk Score" of any Risk Meter can be found on the reporting page, in the Group Overview at the top (shown below). The link in blue is a count of the "risk accepted" vulnerabilities and clicking it will take you to the Explore page, filtered to view those specific vulnerabilities only.

Source of information:

- How is a risk meter score determined?
- Creating a Custom Field
- Reporting on your "True Risk Score"