CSE Information

Customer Success Team

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

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

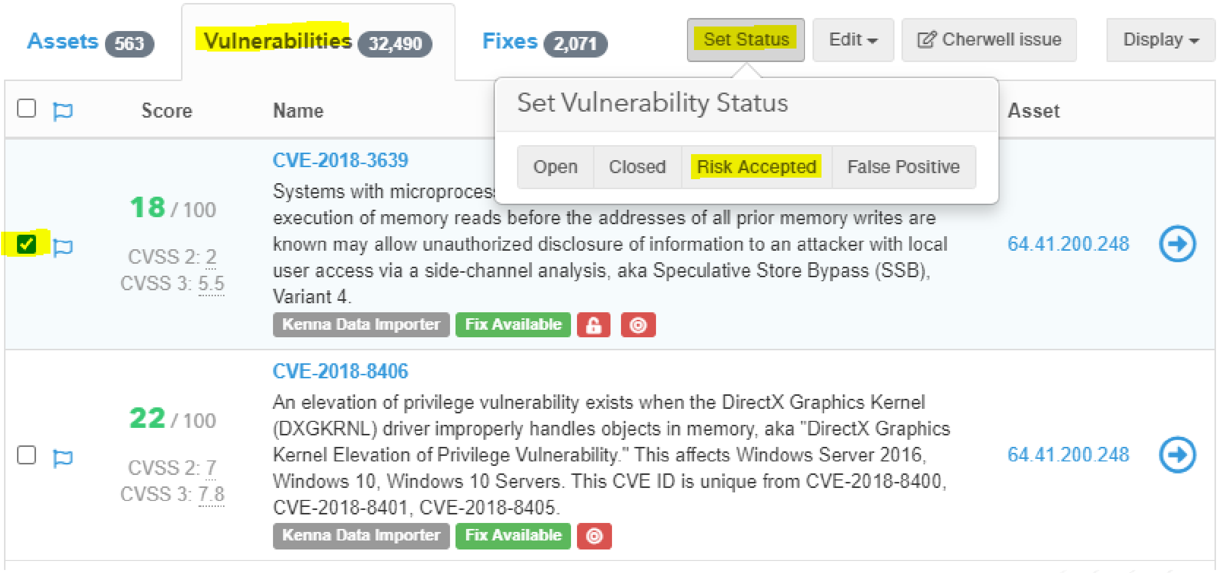
In Kenna, all vulnerabilities have 4 possible statuses: Open, Closed, Risk Accepted, & False Positive, and there are a few places from where you can change the vulnerability status.

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"



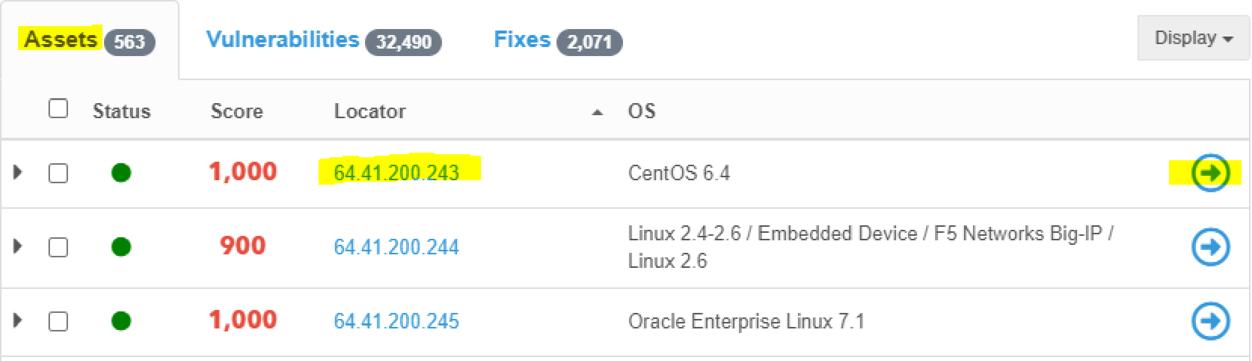
CVE-2018-3639

Systems with microproces execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka Speculative Store Bypass (SSB), Variant 4.

CVE-2018-8406

An elevation of privilege vulnerability exists when the DirectX Graphics Kernel (DXGKRNL) driver improperly handles objects in memory, aka "DirectX Graphics Kernel Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8400, CVE-2018-8401, CVE-2018-8405.

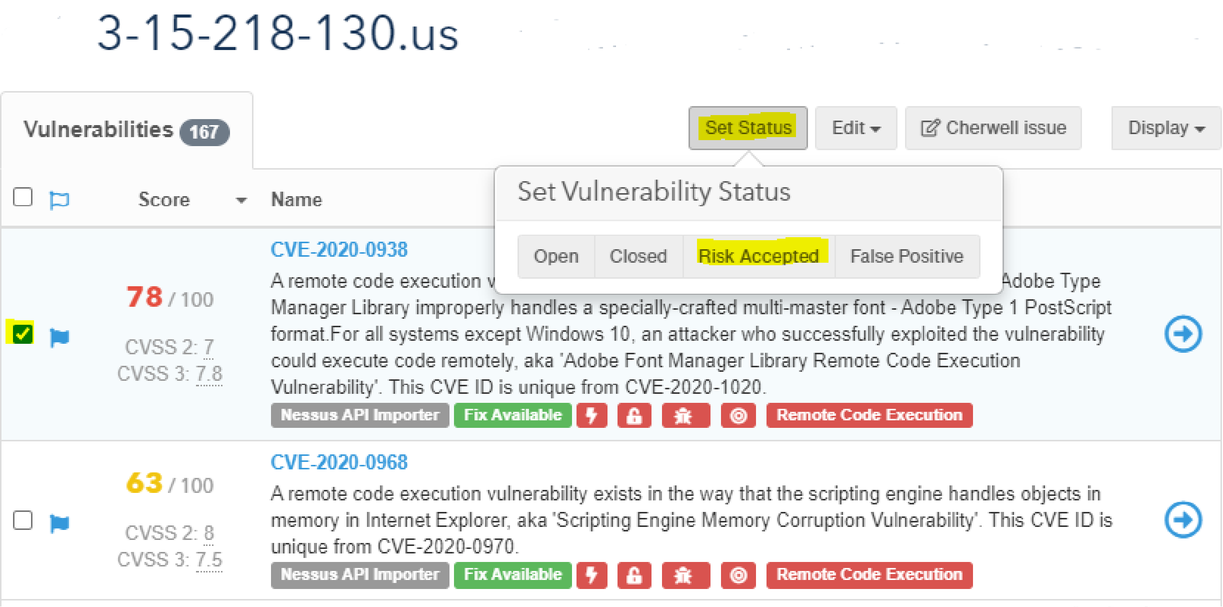
- Directly from the asset's page:
  - From the Explore page, you can either click on the asset's name or in the blue arrow at the right side of the asset's information:



Assets 563 | Vulnerabilities 32,490 | Fixes 2,071 | Display

	□	Status	Score	Locator	OS
▸	□	●	1,000	64.41.200.243	CentOS 6.4
▸	□	●	900	64.41.200.244	Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP / Linux 2.6
▸	□	●	1,000	64.41.200.245	Oracle Enterprise Linux 7.1

  - 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:



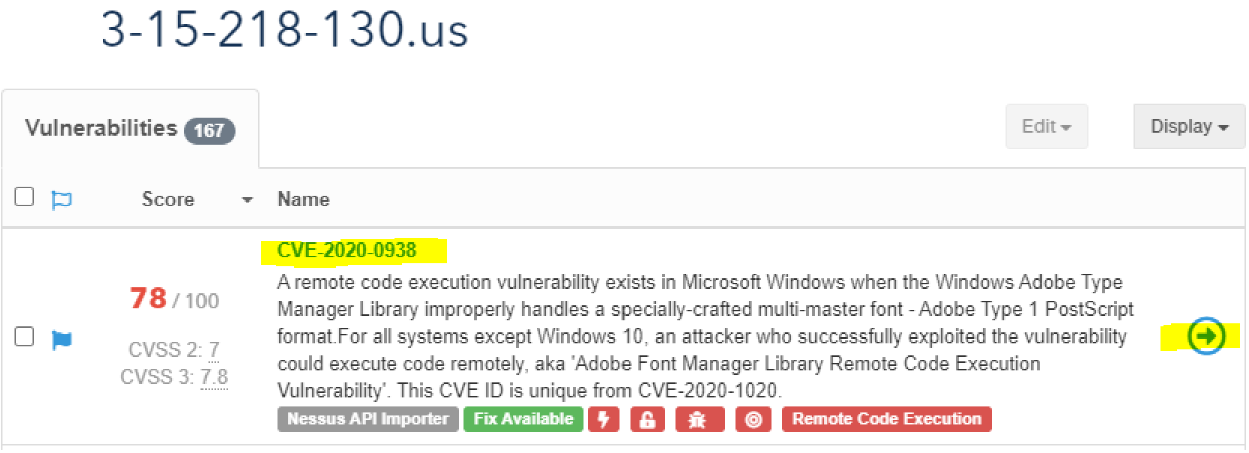
3-15-218-130.us

Vulnerabilities 167 | Set Status | Edit | Cherwell issue | Display

Set Vulnerability Status: Open | Closed | Risk Accepted | False Positive

□	Score	Name
☑	78 / 100 CVSS 2: 7 CVSS 3: 7.8	CVE-2020-0938 A remote code execution v … Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format.For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Adobe Font Manager Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1020. Nessus API Importer · Fix Available · Remote Code Execution
□	63 / 100 CVSS 2: 8 CVSS 3: 7.5	CVE-2020-0968 A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2020-0970. Nessus API Importer · Fix Available · Remote Code Execution

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

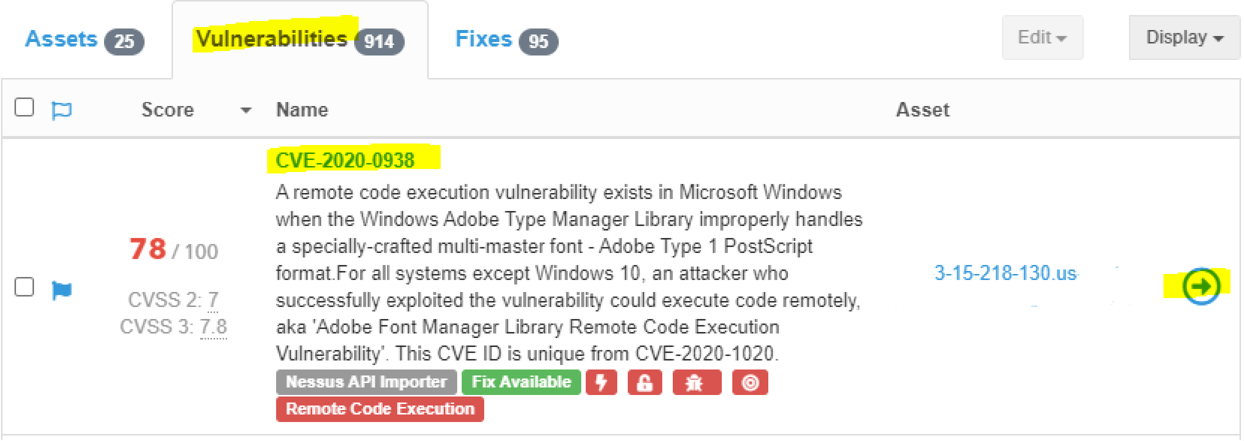


3-15-218-130.us

Vulnerabilities 167

□	Score	Name
□	78 / 100 CVSS 2: 7 CVSS 3: 7.8	CVE-2020-0938 A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format.For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Adobe Font Manager Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1020. Nessus API Importer · Fix Available · Remote Code Execution

Figure 1-Asset's Page

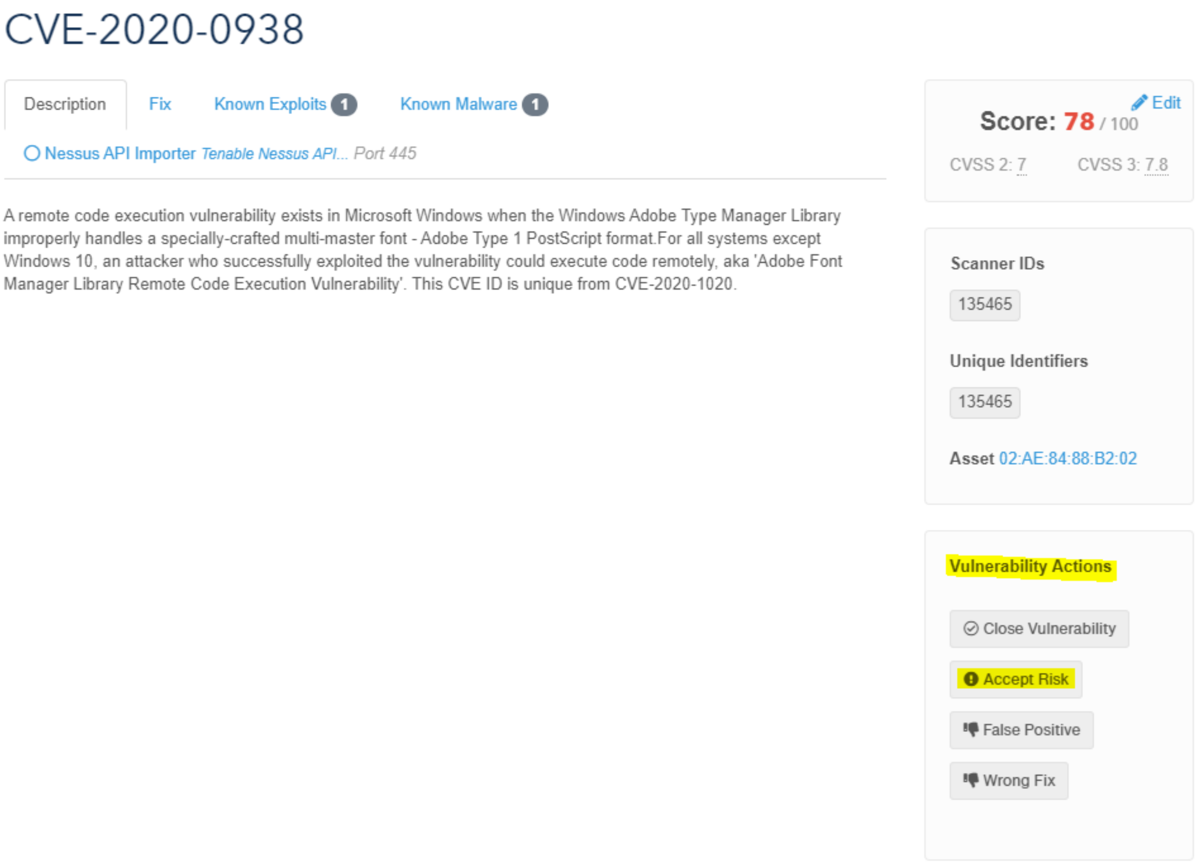


Assets 25 · Vulnerabilities 914 · Fixes 95

□	Score	Name	Asset
□	78 / 100 CVSS 2: 7 CVSS 3: 7.8	CVE-2020-0938 A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format.For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Adobe Font Manager Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1020. Nessus API Importer · Fix Available · Remote Code Execution	3-15-218-130.us

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"



CVE-2020-0938

Description | Fix | Known Exploits 1 | Known Malware 1

○ Nessus API Importer *Tenable Nessus API... Port 445*

A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format.For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Adobe Font Manager Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1020.

Edit

Score: 78 / 100

CVSS 2: 7 CVSS 3: 7.8

Scanner IDs

135465

Unique Identifiers

135465

Asset 02:AE:84:88:B2:02

Vulnerability Actions

Close Vulnerability

Accept Risk

False Positive

Wrong Fix

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.

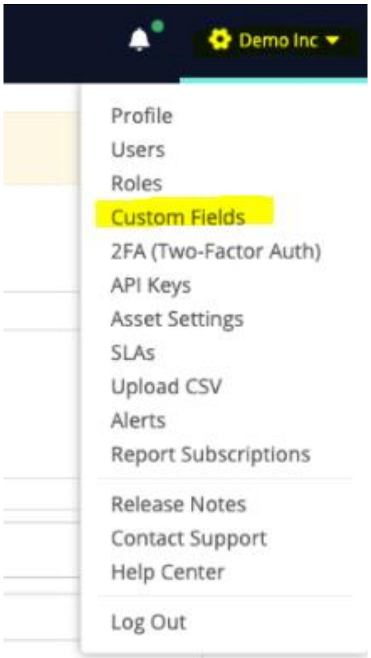
Creating Custom Field:

There are three types of custom fields:

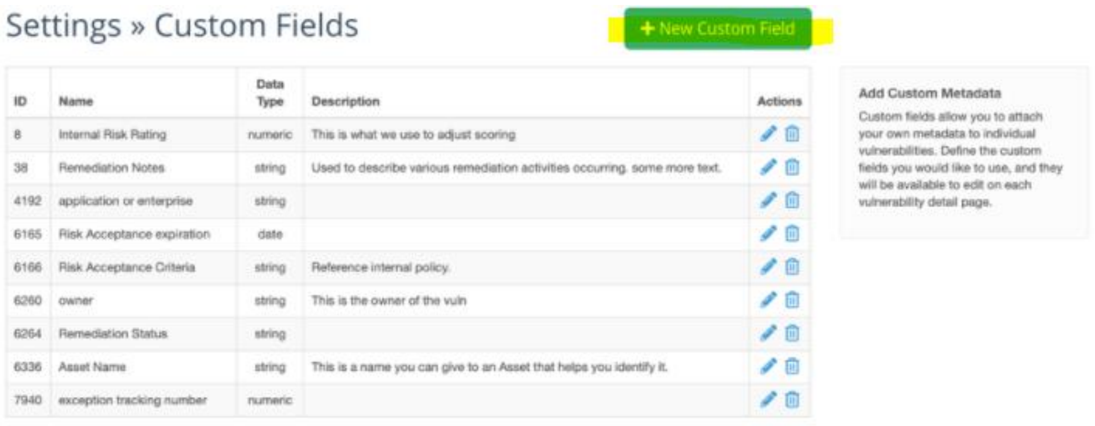
- Text Fields
  - Text fields support up to 2000 characters of text. This can be used for additional notes, marking an Owner of a vulnerability, or any other text based data.
- Date Fields
  - Date fields support a calendar date. When editing a date based custom field, a calendar popup will appear when 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.



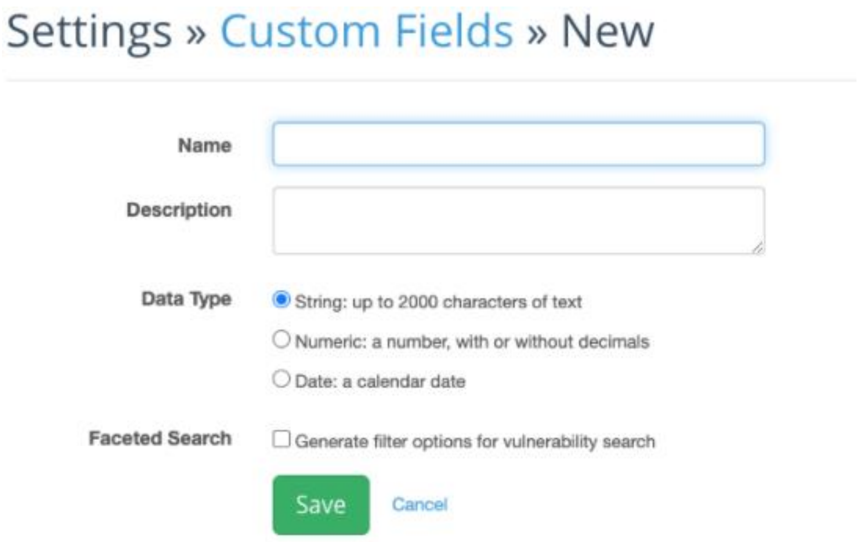
Settings » Custom Fields

ID	Name	Data Type	Description	Actions
8	Internal Risk Rating	numeric	This is what we use to adjust scoring	✎ 🗑
38	Remediation Notes	string	Used to describe various remediation activities occurring. some more text.	✎ 🗑
4192	application or enterprise	string		✎ 🗑
6165	Risk Acceptance expiration	date		✎ 🗑
6166	Risk Acceptance Criteria	string	Reference internal policy.	✎ 🗑
6260	owner	string	This is the owner of the vuln	✎ 🗑
6264	Remediation Status	string		✎ 🗑
6336	Asset Name	string	This is a name you can give to an Asset that helps you identify it.	✎ 🗑
7940	exception tracking number	numeric		✎ 🗑

Add Custom Metadata

Custom fields allow you to attach your own metadata to individual vulnerabilities. Define the custom fields you would like to use, and they will be available to edit on each vulnerability detail page.

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



Settings » Custom Fields » New

Name	
Description	
Data Type	● String: up to 2000 characters of text ○ Numeric: a number, with or without decimals ○ Date: a calendar date
Faceted Search	□ Generate filter options for vulnerability search

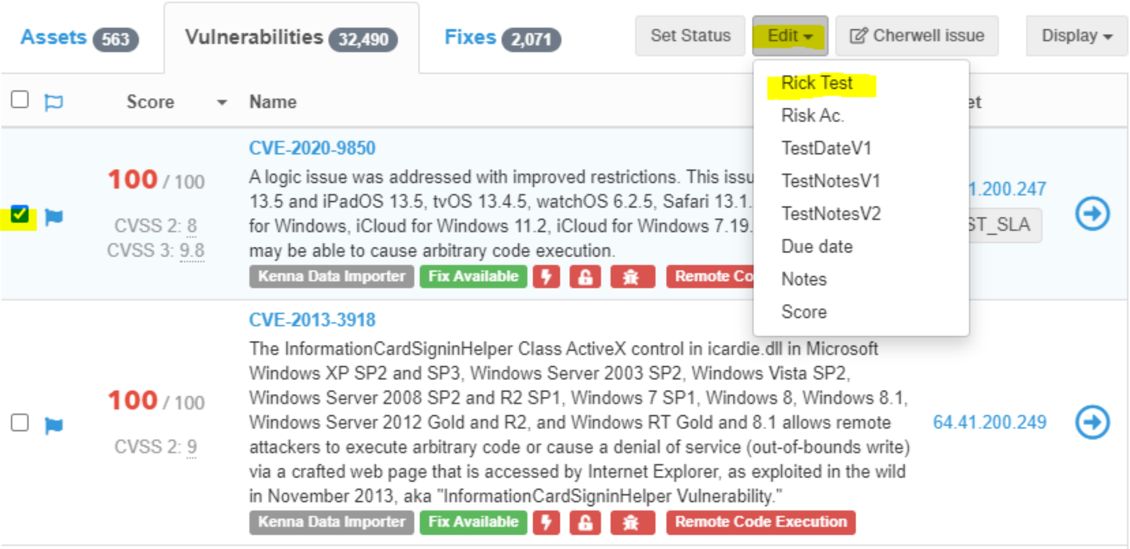
Note: For each unique entry in a custom field creates a new checkbox in Explore. For example, if you have four unique dates/numbers/text strings, it will create four checkboxes.

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.



☑ 100 / 100 CVSS 2: 8 CVSS 3: 9.8

CVE-2020-9850

A logic issue was addressed with improved restrictions. This issu
13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.
for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19.
may be able to cause arbitrary code execution.

1.200.247 ST_SLA

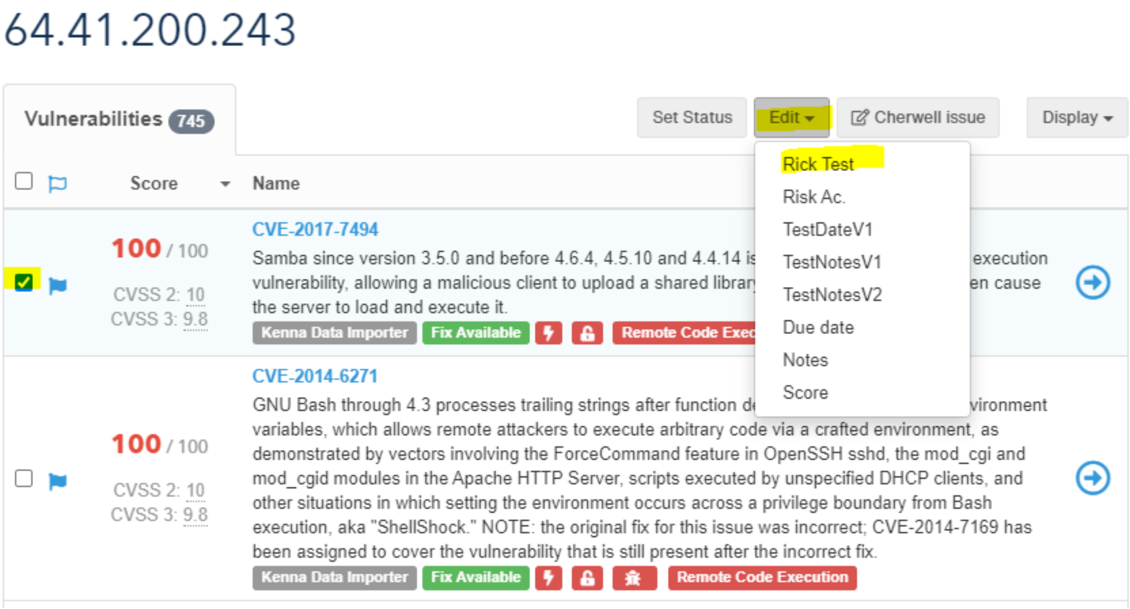
□ 100 / 100 CVSS 2: 9

CVE-2013-3918

The InformationCardSigninHelper Class ActiveX control in icardie.dll in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds write) via a crafted web page that is accessed by Internet Explorer, as exploited in the wild in November 2013, aka "InformationCardSigninHelper Vulnerability."

64.41.200.249

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.



☑ 100 / 100 CVSS 2: 10 CVSS 3: 9.8

CVE-2017-7494

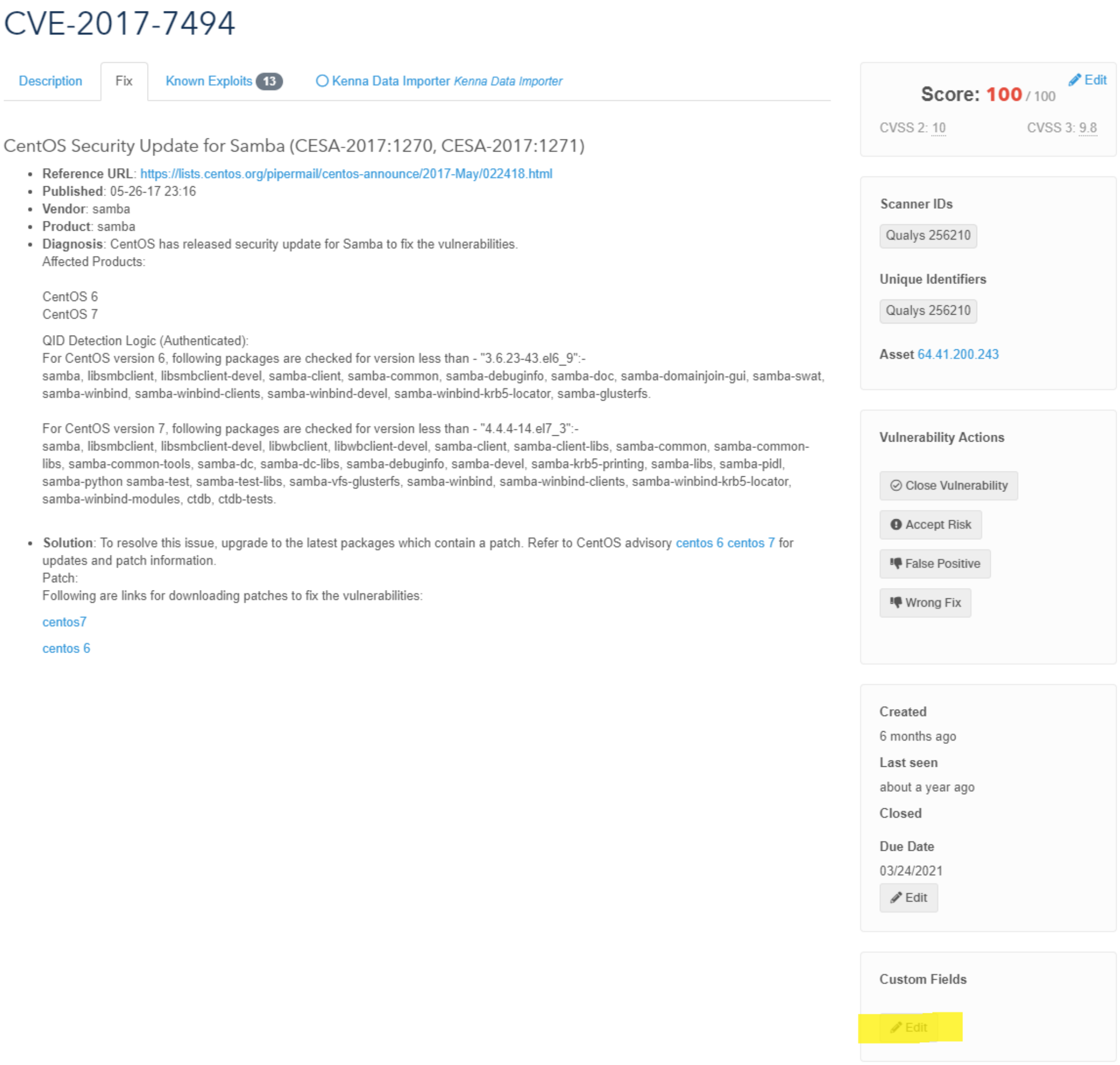
Samba since version 3.5.0 and before 4.6.4, 4.5.10 and 4.4.14 is execution
vulnerability, allowing a malicious client to upload a shared librar en cause
the server to load and execute it.

□ 100 / 100 CVSS 2: 10 CVSS 3: 9.8

CVE-2014-6271

GNU Bash through 4.3 processes trailing strings after function d vironment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock." NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.

3. From the Vulnerability's page



CVE-2017-7494

CentOS Security Update for Samba (CESA-2017:1270, CESA-2017:1271)

- **Reference URL**: https://lists.centos.org/pipermail/centos-announce/2017-May/022418.html
- **Published**: 05-26-17 23:16
- **Vendor**: samba
- **Product**: samba
- **Diagnosis**: CentOS has released security update for Samba to fix the vulnerabilities.
  Affected Products:

  CentOS 6
  CentOS 7

  QID Detection Logic (Authenticated):
  For CentOS version 6, following packages are checked for version less than - "3.6.23-43.el6_9":-
  samba, libsmbclient, libsmbclient-devel, samba-client, samba-common, samba-debuginfo, samba-doc, samba-domainjoin-gui, samba-swat, samba-winbind, samba-winbind-clients, samba-winbind-devel, samba-winbind-krb5-locator, samba-glusterfs.

  For CentOS version 7, following packages are checked for version less than - "4.4.4-14.el7_3":-
  samba, libsmbclient, libsmbclient-devel, libwbclient, libwbclient-devel, samba-client, samba-client-libs, samba-common, samba-common-libs, samba-common-tools, samba-dc, samba-dc-libs, samba-debuginfo, samba-devel, samba-krb5-printing, samba-libs, samba-pidl, samba-python samba-test, samba-test-libs, samba-vfs-glusterfs, samba-winbind, samba-winbind-clients, samba-winbind-krb5-locator, samba-winbind-modules, ctdb, ctdb-tests.

- **Solution**: To resolve this issue, upgrade to the latest packages which contain a patch. Refer to CentOS advisory centos 6 centos 7 for updates and patch information.
  Patch:
  Following are links for downloading patches to fix the vulnerabilities:

  centos7

  centos 6

Score: **100** / 100
CVSS 2: 10 CVSS 3: 9.8

Scanner IDs
Qualys 256210

Unique Identifiers
Qualys 256210

Asset 64.41.200.243

Vulnerability Actions

Created
6 months ago
Last seen
about a year ago
Closed

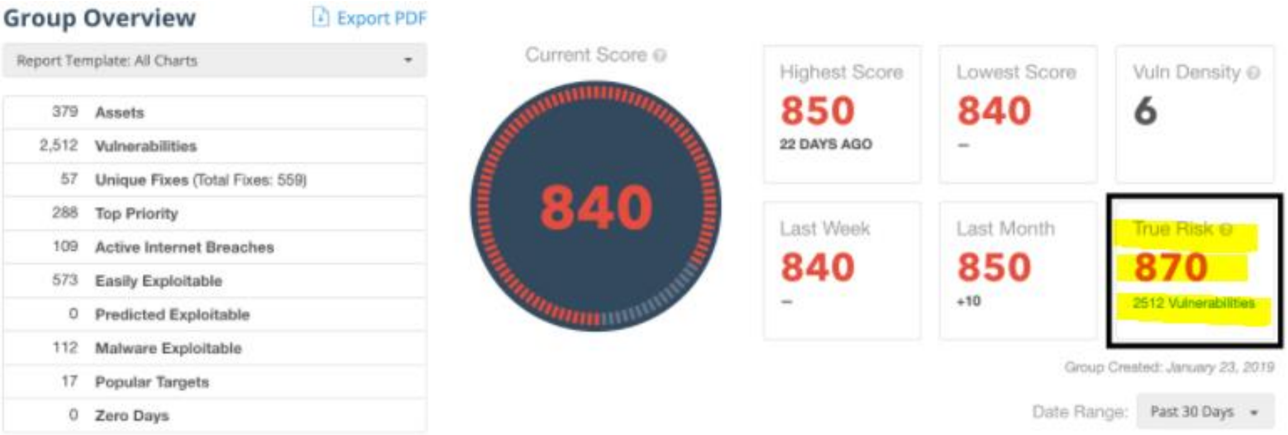
Due Date
03/24/2021

Custom Fields

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.



Group Overview

Export PDF

Report Template: All Charts

379	Assets
2,512	Vulnerabilities
57	Unique Fixes (Total Fixes: 559)
288	Top Priority
109	Active Internet Breaches
573	Easily Exploitable
0	Predicted Exploitable
112	Malware Exploitable
17	Popular Targets
0	Zero Days

Current Score: 840

Highest Score 850 22 DAYS AGO	Lowest Score 840 –	Vuln Density 6
Last Week 840 –	Last Month 850 +10	True Risk 870 2512 Vulnerabilities

Group Created: January 23, 2019

Date Range: Past 30 Days

Source of information:

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