KENNA Security

All Things Vulnerabilities

Caleb Eckenwiler

Kenna Security, Customer Success Manager

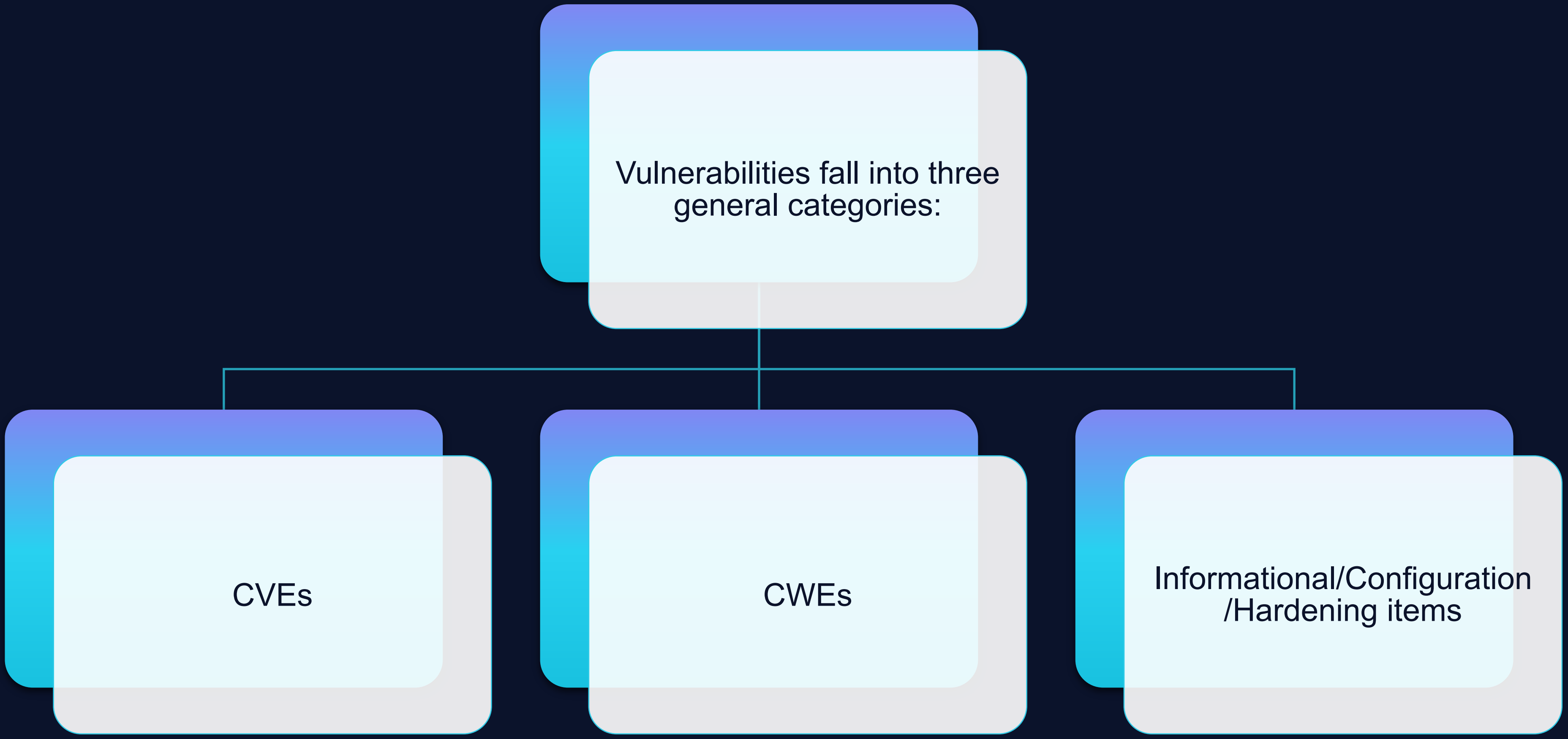
10/23/2020

All Things Vulnerabilities

Agenda

- Vulnerability Basics
- Vulnerability Statuses
- How Vulnerabilities get closed within Kenna
- Using Custom Fields for False Positive & Risk Accepted Vulnerabilities
- Vulnerability Details and Features
- Querying for Vulnerability Score Change History

Vulnerability Categorization



Vulnerabilities fall into three general categories:

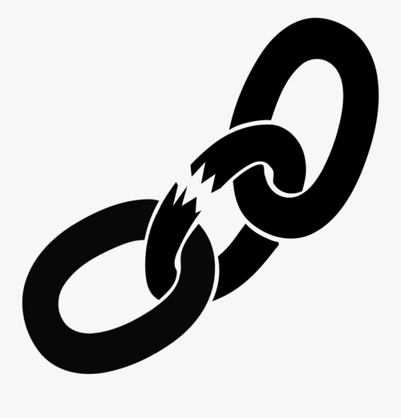
CVEs

CWEs

Informational/Configuration /Hardening items

KENNA Security

Vulnerability Basics: CVEs



- What is a vulnerability?

  A vulnerability is a weakness which can be exploited by a bad-actor to allow unauthorized access, elevation of privileges, denial of service, etc.

- How are vulnerabilities discovered?

  A multitude of vulnerabilities are discovered each year by Security Researchers, Security Practitioners, Software Vendors, and bad actors.

- How is a vulnerability identified?

  Vulnerabilities that are discovered and confirmed are given an identification. The Common Vulnerabilities and Exposures list or CVEs are identified by the following format: “CVE-YYYY-#” where YYYY is the year the ID was assigned(or in some cases the year the CVE was made public), and the number is the order in which the vulnerability was found. Each year, the list restarts at 1.

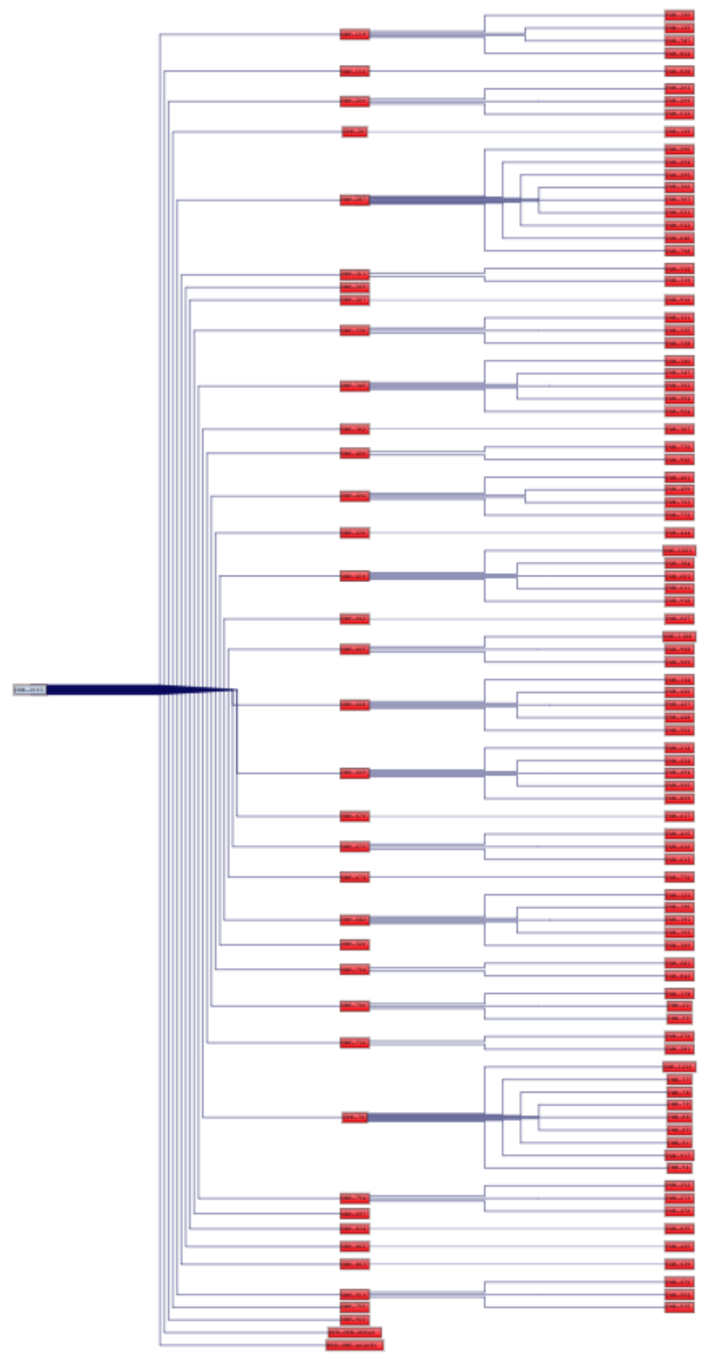
- How is a vulnerability scored?

  Vulnerabilities that receive a CVE will typically receive a CVSS or Common Vulnerability Scoring System score on a scale of 1-10. CVSS is a free and open industry standard for assessing the severity of a vulnerability if it were to be exploited.

KENNA
Security

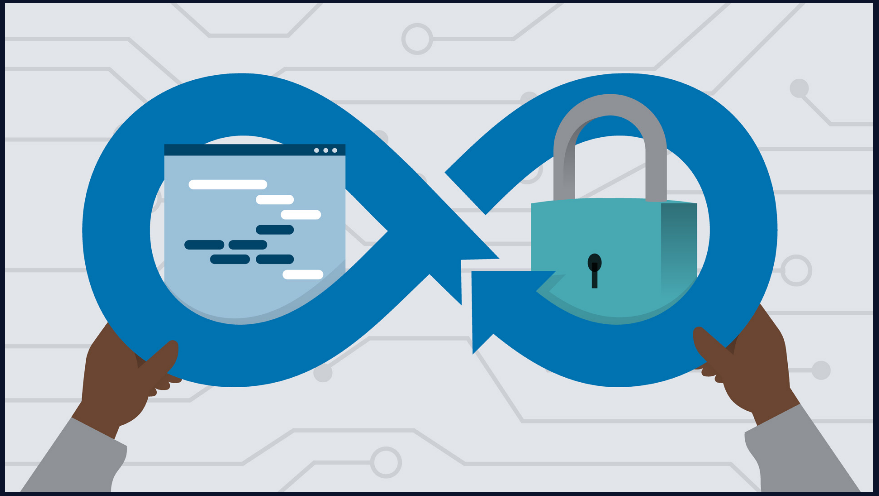
Common Weakness Enumeration Vulnerabilities

- CWEs or Common Weakness Enumeration vulnerabilities typically refer to weaknesses in Code, Design, or System Architecture.
- CWEs are more hierarchical than CVEs, and allows for multiple levels of abstraction.
- Think of CWEs as classes of vulnerabilities, and CVEs as specific instances of vulnerability for certain products and/or systems.



Portion of CWE Structure

Configuration Vulnerabilities

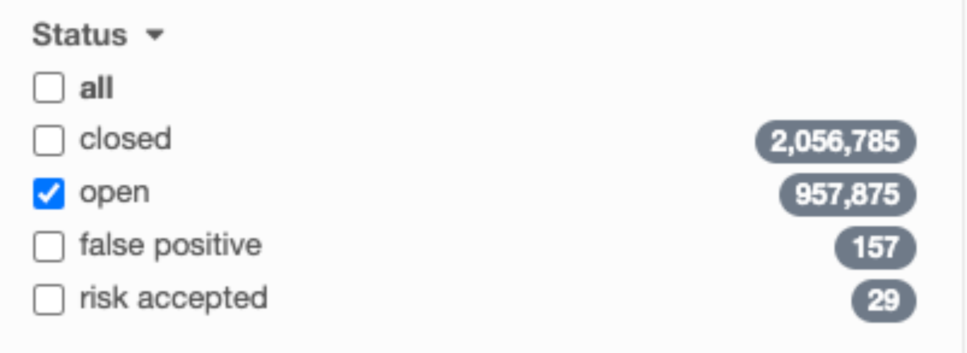


- Certain weaknesses exist that are not CVEs but are given initial CVSS scores. These types of issues are typically called informationals, or configuration based vulnerabilities.

Examples include: End of Life systems, Self-Signed certificates, Default passwords, Deprecated SSH Cryptographic Settings, No Expiration on Administrator Password, Missing HTTP Security Header, SSL/TLS issues, etc.

KENNA Security

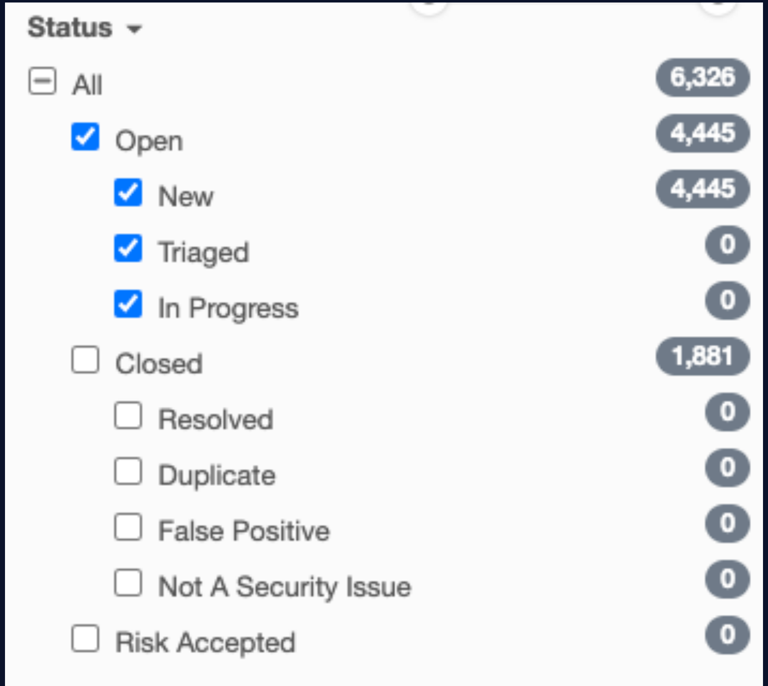
Vulnerability Statuses



Status ▾

- ☐ all
- ☐ closed 2,056,785
- ☑ open 957,875
- ☐ false positive 157
- ☐ risk accepted 29

- Open
- Closed
- False Positive
- Risk Accepted



Status ▾

- ⊟ All 6,326
  - ☑ Open 4,445
    - ☑ New 4,445
    - ☑ Triaged 0
    - ☑ In Progress 0
  - ☐ Closed 1,881
    - ☐ Resolved 0
    - ☐ Duplicate 0
    - ☐ False Positive 0
    - ☐ Not A Security Issue 0
  - ☐ Risk Accepted 0

- Open
  - New
  - In Progress
  - Triaged
- Closed
  - Resolved
  - Duplicate
  - False Positive
  - Not a Security Issue
- Risk Accepted

Demo Time!

- Asset Statuses and where to edit them

How Vulnerabilities are Closed in Kenna

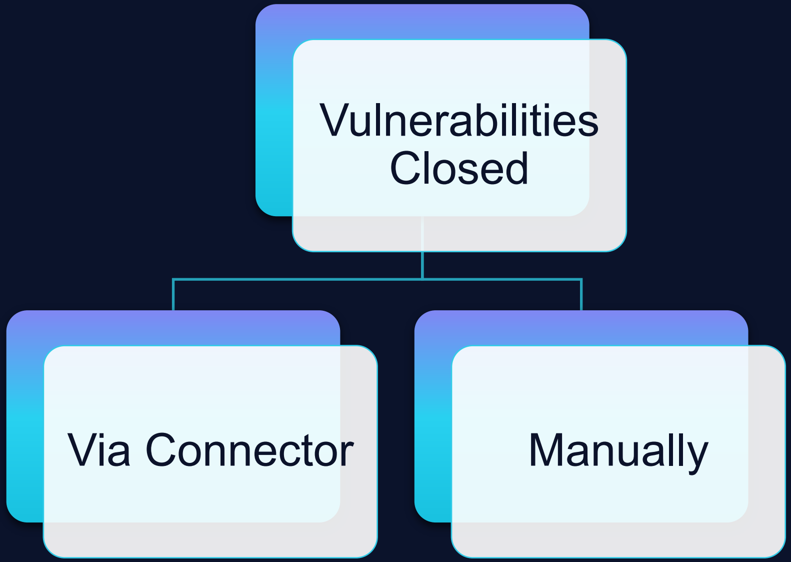
There are a couple caveats to each method of closing vulnerabilities.

Vulnerabilities Closed Manually

- Vulnerabilities that are manually closed have a flag on the back-end that gets set once the vuln is marked closed. If this flag is set, the vulnerability will never be reopened by the scanner. The platform interprets the manual action as the single source of truth and will keep the vulnerability closed.
- To remove said flag, you can ask Support, or simply re-set the vulnerability to open, after which the connector will pick it back up in the next run, and if the vuln is closed, set the status to Closed, or if it is open, leave it Open.
- If the vulnerability isn't truly closed, this information will not be reflected in Kenna properly, since the manual override will not allow the vulnerability to return to an "Open" status.

Vulnerabilities Closed Automatically (Via Connector)

- Vulnerabilities that are re-scanned by the Vuln Scanner and reported closed will automatically be closed in Kenna once the Connector runs and imports that information.
- If a vulnerability is seen by more than one scanner, it must be reported closed by *each* scanner before it will reflect the Closed status in Kenna.



KENNA Security

False Positive & Risk Accepted Vulnerabilities

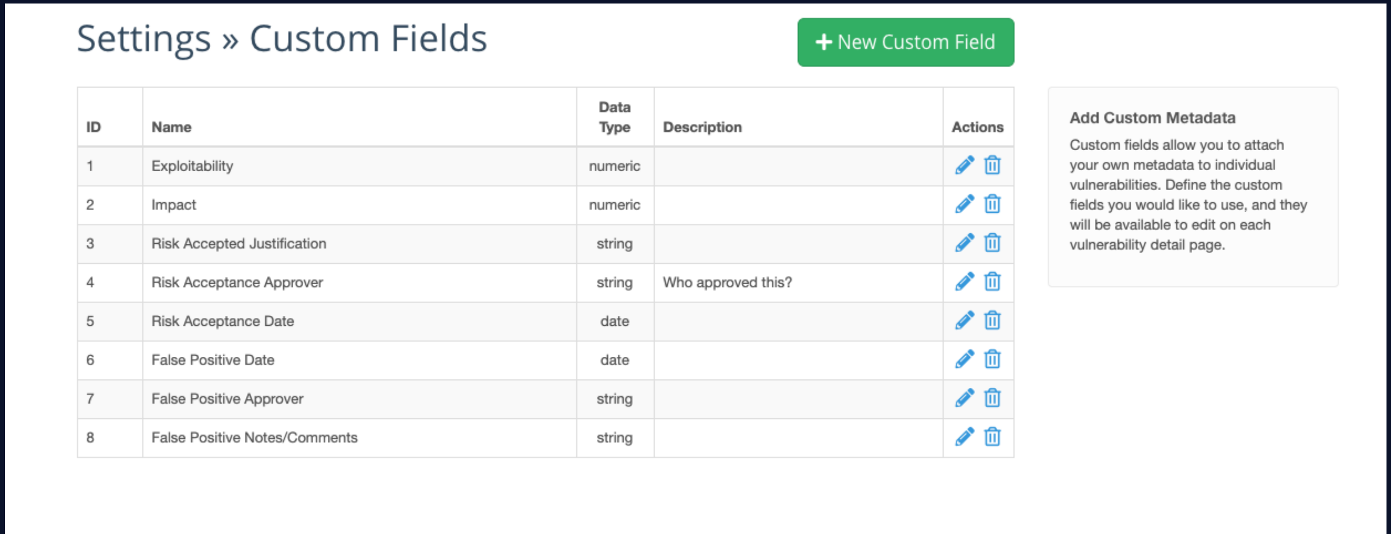
We live in an imperfect world, which means that at some point, you will be wrong. This is no different for vulnerability management. At some point, you will have a vulnerability reported that is a false positive. The best step to take, is to then accurately identify the vulnerability as a false positive, so that remediation teams don’t spend time chasing their tails trying to patch a vulnerability that isn’t there.

Similarly, if you are managing assets that have software that require specific versions, or the Team judges the Risk to be lower than reported due to various reasons, vulnerabilities can be identified as Risk Accepted.

Tracking these vulnerabilities properly is important for not only security, but also for auditory compliance, and the goal of maintaining good data.

Using Custom Fields for False Positive & Risk Accepted Vulnerabilities

- In order to track Risk Accepted and False Positive vulnerabilities within Kenna, you will need to leverage a couple of custom fields.
- Custom Fields allow you to attach your own metadata to individual vulnerabilities.
- Typically, we suggest three fields per status (ex. w/ RA status)
  - Risk Accepted Date
  - Risk Accepted Approver
  - Risk Accepted Notes
- These fields would be replicated for False Positives:
  - False Positive Date
  - False Positive Approver
  - False Positive Notes



Settings » Custom Fields

ID	Name	Data Type	Description	Actions
1	Exploitability	numeric		✎ 🗑
2	Impact	numeric		✎ 🗑
3	Risk Accepted Justification	string		✎ 🗑
4	Risk Acceptance Approver	string	Who approved this?	✎ 🗑
5	Risk Acceptance Date	date		✎ 🗑
6	False Positive Date	date		✎ 🗑
7	False Positive Approver	string		✎ 🗑
8	False Positive Notes/Comments	string		✎ 🗑

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.

KENNA
Security

Demo Time!

- Reviewing Custom Fields

KENNA
Security

Vulnerability Details

- The Vulnerability Details page provides more information about the specific vuln:
  - Score (Kenna and CVSS)
  - Description
  - Fix
  - Known Exploits
  - Scanner(s) the vuln was imported from
- You can also perform certain tasks in the Vuln Details view
  - Change Status
  - Change Due Date
  - Edit Custom Fields

Demo Time!

- Reviewing the Vulnerability Details page

Querying the API for Vulnerability Score History

- https://apidocs.kennasecurity.com/reference#show-cve-history
- Simple -curl command
- Customers who have purchased Kenna.VI+ may access any CVE. Customers who have not purchased the Kenna.VI+ product may only access CVEs that correspond to vulnerabilities within their instance.

KENNA
Security

Q & A

KENNA
Security

Thank you

Caleb Eckenwiler

Kenna Security, CSM