CISCO
SECURE

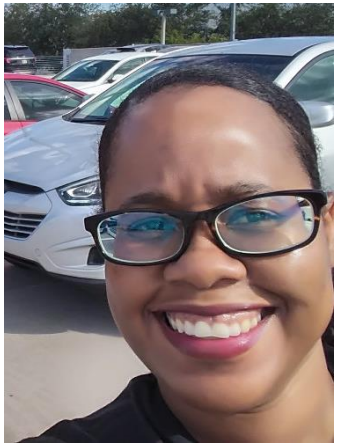
All Things Vulnerabilities

May 23, 2023

Presenters:

Lidia Attalla

Customer Success Engineer



Ren Ferril

Customer Success Manager

Jamey McGrath

Customer Success Manager

Agenda

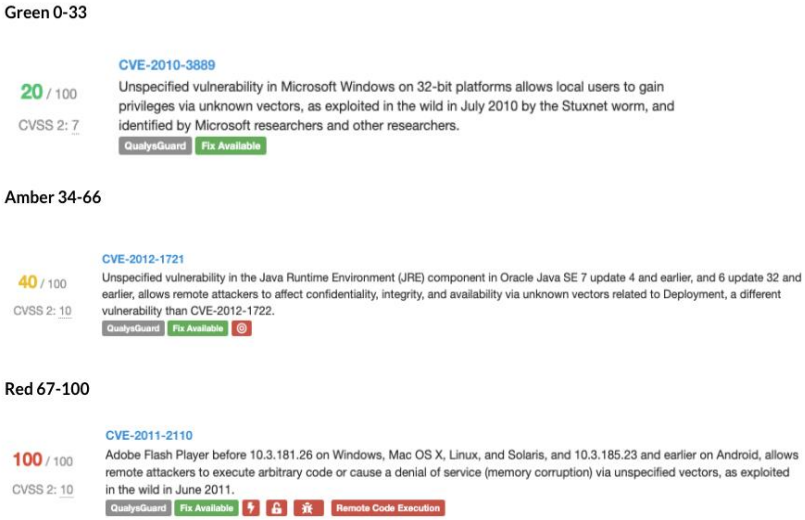
- Vuln basics – what is a vulnerability?
- Vuln Score
- Vuln details page
- Vuln statuses
- How vulns get closed in Kenna
- Using custom fields for false positive/risk acceptance workflow
- Demo and Q&A

Vulnerability Basics

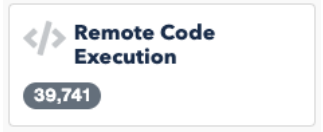
- What is a vulnerability?
  - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source
- How is a vulnerability identified?
  - Vulnerabilities that are discovered and confirmed are given an identification. The Common Vulnerabilities and Exposures list (CVEs) are identified in the following format: "CVE-YYYY-#" where the YYYY is the year the ID was assigned or made public and the # is the order in which the vuln was found.
- How is a vulnerability scored?
  - Vulnerabilities that receive a CVE will typically receive a CVSS (Common Vulnerability Scoring System) score on a scale of 1-10. CVSS is open industry standard for assessing the severity of a vulnerability if it were to be exploited.

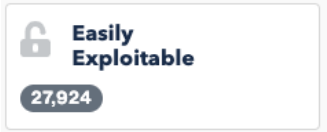
Vulnerability Score

- What is the Kenna Risk Score?
  - A vulnerability score that is applied to each CVE
    - The scores range from 0 – 100
  - Estimates the probability / likelihood of exploitation for that CVE
    - The score could change daily based on many different factors

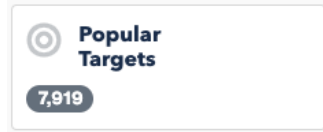


What impacts the Kenna Score?





Active Internet Breach	• Identifies if the vulnerability is actively being breached in the wild • We track the volume and velocity of exploitations by day, week and month
Easily Exploitable	• Vulnerabilities that are included in exploit kits or other public source
Pre NVD-Chatter	• Discussion of this vulnerability 3 or more sources 5 or more times
Malware Exploitable	• Identifying if this vulnerability has pieces of malware associated with it
Predicted Exploitable	• This will tell you if Kenna's algorithm predicts future exploits to develop that would leverage this vulnerability
Remote Code Execution	• Identifies if a vulnerability has remote code execution availability
Popular Target	• Vulnerabilities that are trending popularity across many customers

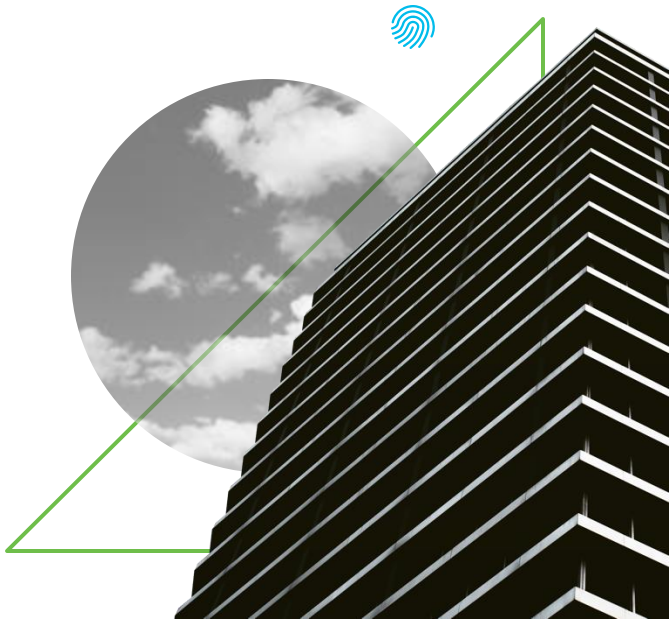


Vulnerability Details Page

- It is this page that provides more information about the specific vulnerability, such:
  - Scanners, Scores, Description, Fixes and Exploits

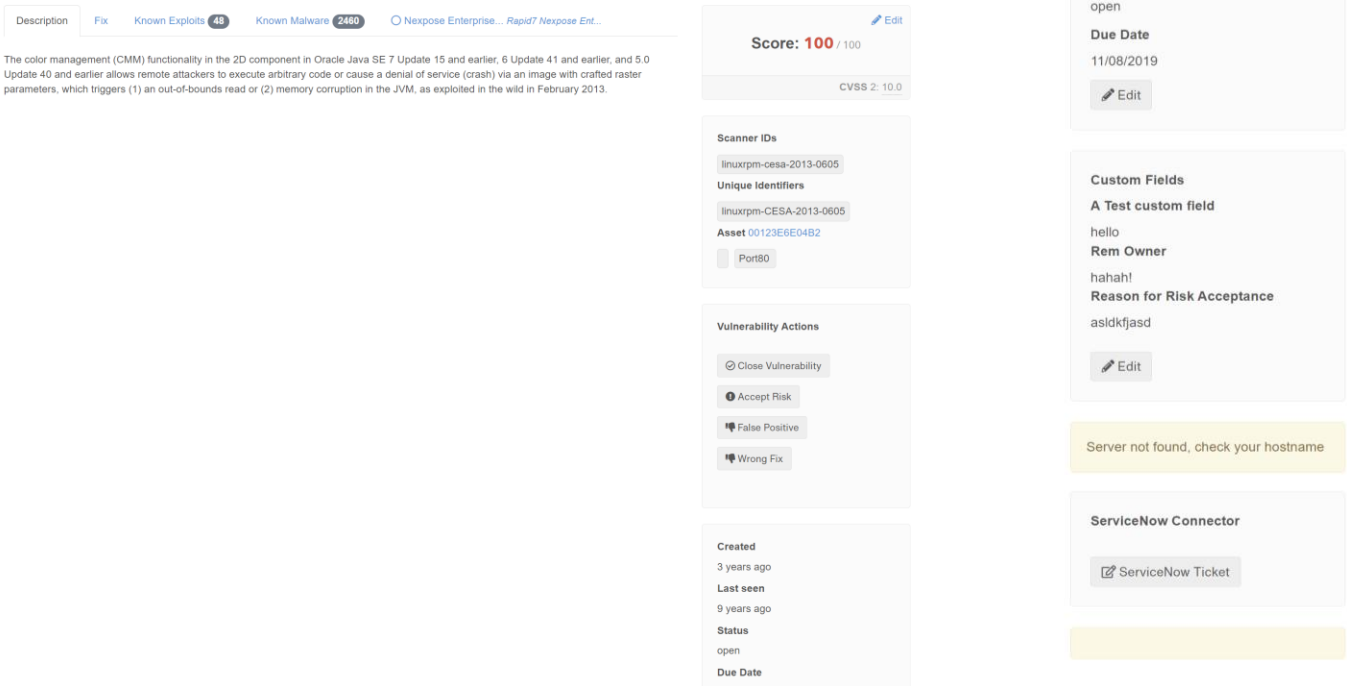
  AND

  Do tasks such as:
  - Status Changes, Editing Custom Fields and Changing Due Dates

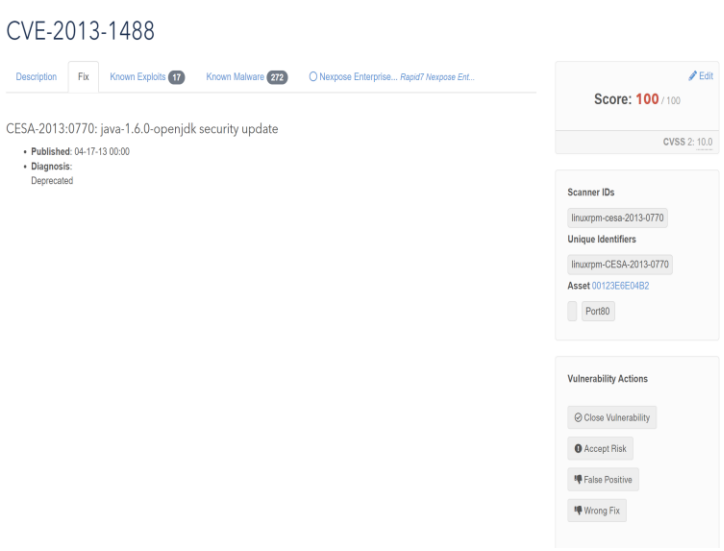


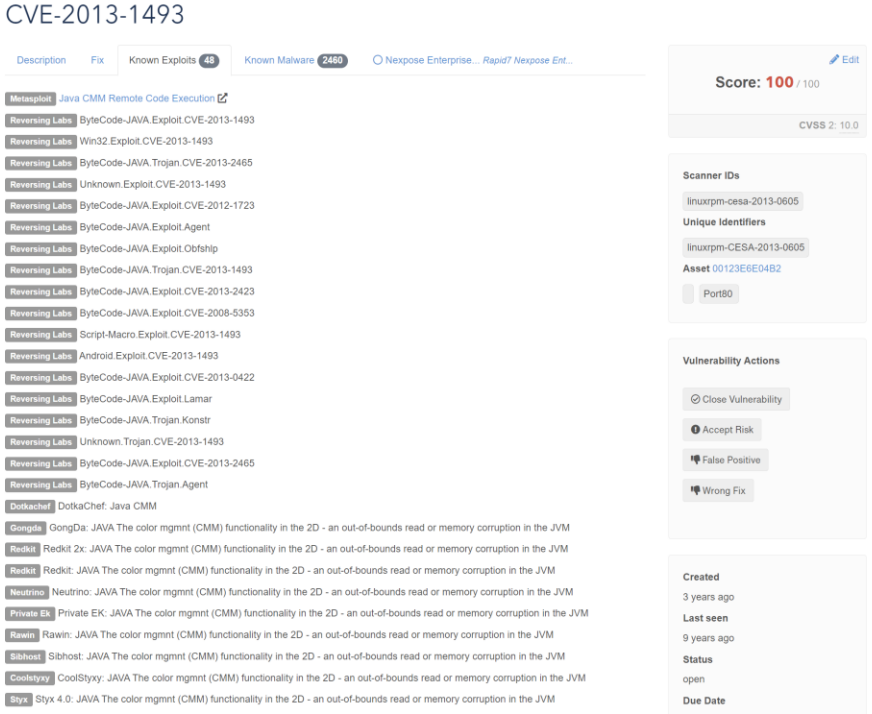
Vulnerability Details Page

CVE-2013-1493



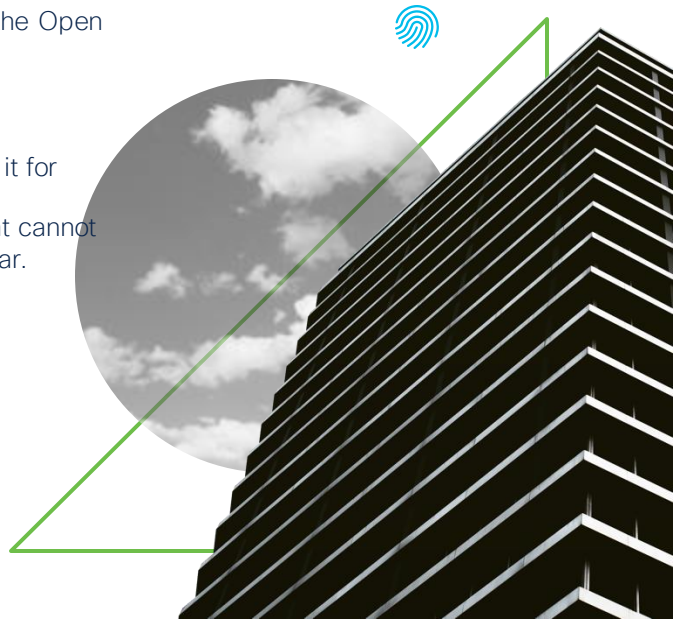
Vulnerability Details Page





Vulnerability Statuses

- Open
  - The vulnerability is still a risk in your organizational data and is available in the Kenna platform for remediation. This is the default status for vulnerabilities.
- Closed
  - The vulnerability has been remediated by your team. Once closed, it is removed from the Open vulnerability view.
- 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.
- False Positive
  - The vulnerability identified in your scan file is not actually a vulnerability.



How Vulnerabilities are Closed

Vulnerabilities are closed either: via Connector or Manually

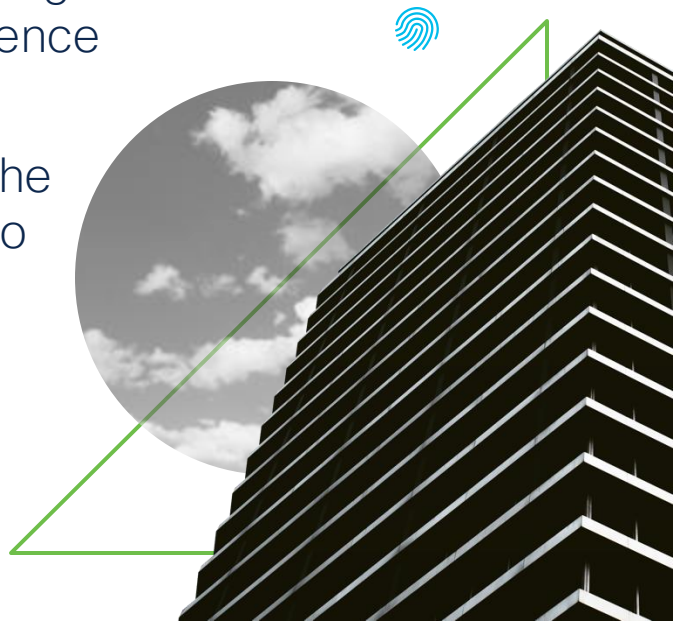
Connector: the connector scans and analyzes which assets are reported closed or still vulnerable after a connector run imports that info.

- Advantage: Makes it much easier to track the state of your vulns over time. No longer affects asset scores or appear on the Explore page.
- Note: if the vuln is seen by more than one scanner, it must be closed by each scanner before it will reflect Closed.

How Vulnerabilities are Closed

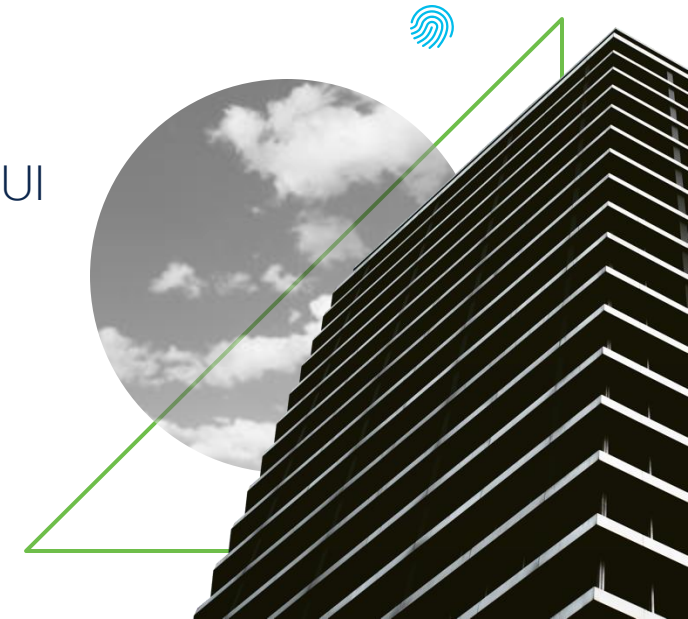
Vulnerabilities are closed either: via Connector or Manually

- Manually: Manual closing generates a back-end flag once marked closed. Human action takes precedence and the vuln will not be reopened by the scanner.
- Able to open a Support ticket to reopen/remove the flag or re-set the vulnerability manually to Open, to be picked up on the next run.



Kenna Custom Field

- What is a Custom field?
- Custom field types
- How to create a custom field
- How to add Data to a custom field
- How to display and manage a custom field in the UI



CISCO
SECURE

Demo Time!

Appreciate your time and patience!

Thank You!