CISCO
SECURE

Kenna Vs Vulnerabilities: What's the score?

February 28, 2023

CISCO The bridge to possible

Presenters:

Katie Conners

Technical Account Manager

Stephanie Deirmentzoglou

Customer Success Manager

Jamey McGrath

Customer Success Operations Specialist

Agenda

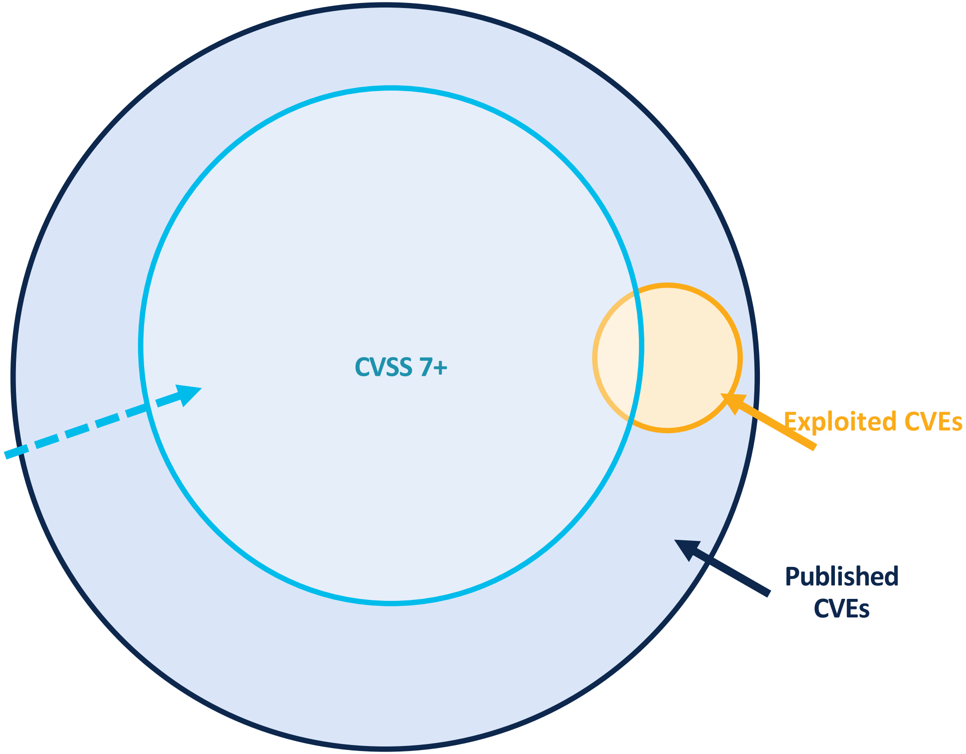
- How does Kenna score vulnerabilities?
- Asset Scoring and Prioritization
- Risk meter score
- Demo
- Q&A

A Wicked Problem

Somewhere between 2-5% of CVEs are (detected as) exploited in the wild.

How do we prioritize these?

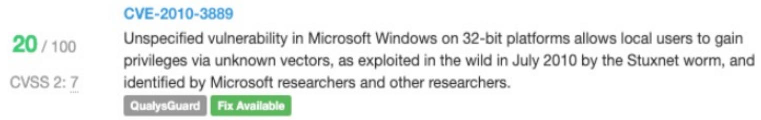
How does CVSS help?



What is the Kenna 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

Green 0-33



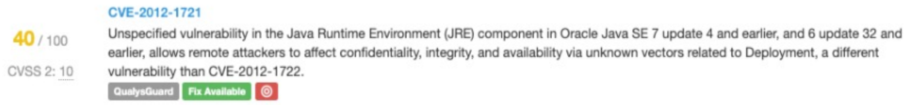
20 / 100

CVSS 2: 7

CVE-2010-3889

Unspecified vulnerability in Microsoft Windows on 32-bit platforms allows local users to gain privileges via unknown vectors, as exploited in the wild in July 2010 by the Stuxnet worm, and identified by Microsoft researchers and other researchers.

Amber 34-66



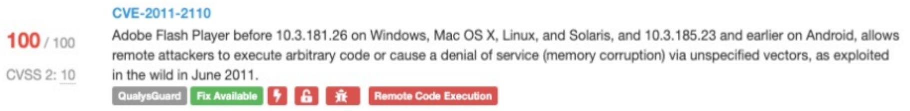
40 / 100

CVSS 2: 10

CVE-2012-1721

Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 update 4 and earlier, and 6 update 32 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Deployment, a different vulnerability than CVE-2012-1722.

Red 67-100



100 / 100

CVSS 2: 10

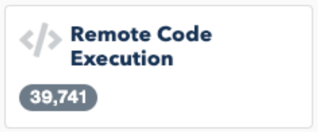
CVE-2011-2110

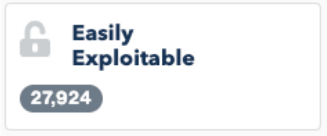
Adobe Flash Player before 10.3.181.26 on Windows, Mac OS X, Linux, and Solaris, and 10.3.185.23 and earlier on Android, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as exploited in the wild in June 2011.

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

Predicted Exploitable
1,040


Remote Code Execution
39,741


Easily Exploitable
27,924

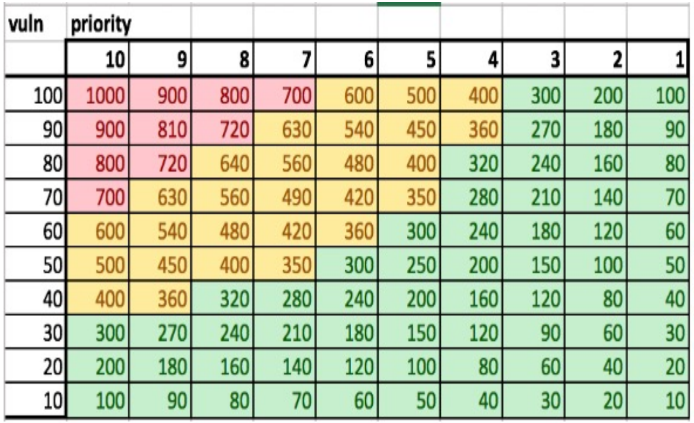
Active Net Breaches
1,915

Malware Exploitable
1,753

Popular Targets
7,919

Asset Priority

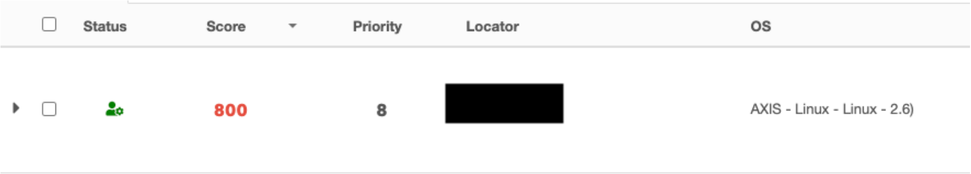
- Kenna allows customers to prioritize assets within the platform
- Asset prioritization allows customers to identify and manage assets that are critical to the organization
- The asset priority range is 0 – 10
- We do not advise customers to set prioritization below a 7



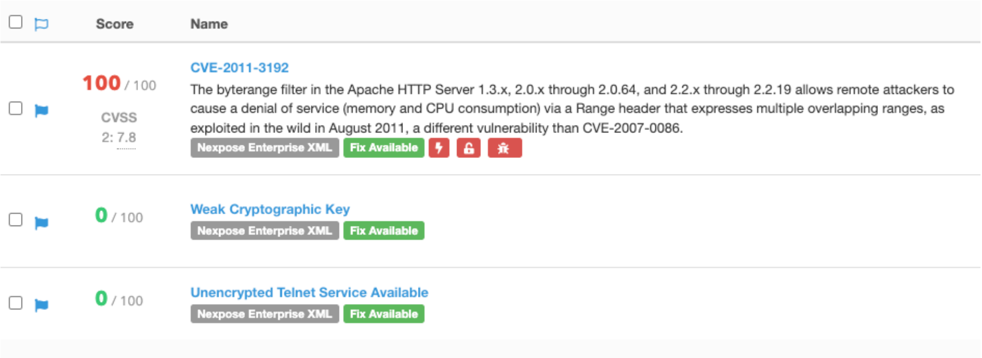
vuln	priority									
	10	9	8	7	6	5	4	3	2	1
100	1000	900	800	700	600	500	400	300	200	100
90	900	810	720	630	540	450	360	270	180	90
80	800	720	640	560	480	400	320	240	160	80
70	700	630	560	490	420	350	280	210	140	70
60	600	540	480	420	360	300	240	180	120	60
50	500	450	400	350	300	250	200	150	100	50
40	400	360	320	280	240	200	160	120	80	40
30	300	270	240	210	180	150	120	90	60	30
20	200	180	160	140	120	100	80	60	40	20
10	100	90	80	70	60	50	40	30	20	10

Kenna Asset Score

- Kenna applies a score to assets
- The score ranges from 0 – 1000
- The asset score is calculated by the highest level vulnerability multiplied by the asset priority
- Kenna will apply a 200 point bump to an asset score if we think its external
- An IP other than 10.*, 172.16.0.0 – 172.31.255.255 and 192.168.* to be external



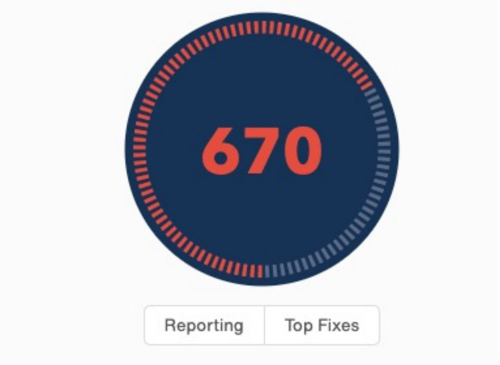
□	Status	Score	Priority	Locator	OS
□		800	8	[redacted]	AXIS - Linux - Linux - 2.6)



□	Score	Name
□	100 / 100 CVSS 2: 7.8	CVE-2011-3192 The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086. Nexpose Enterprise XML · Fix Available
□	0 / 100	Weak Cryptographic Key Nexpose Enterprise XML · Fix Available
□	0 / 100	Unencrypted Telnet Service Available Nexpose Enterprise XML · Fix Available

Risk Meter Score

- Kenna allows you to collate and save assets together in logical groups
- Each saved search (or group) is allocated a risk meter score
- The risk meter score ranges from 0 – 1000
- This is calculated by taking the average of the asset risk score within the group excluding 0 scored assets



- Green = Score between 0 - 333
- Yellow = Score between 334 - 666
- Red = Score between 667 - 1000

CISCO SECURE

Demo Time!

CISCO The bridge to possible

Ensuring Your Success

Appreciate your time and patience!

Thank You!