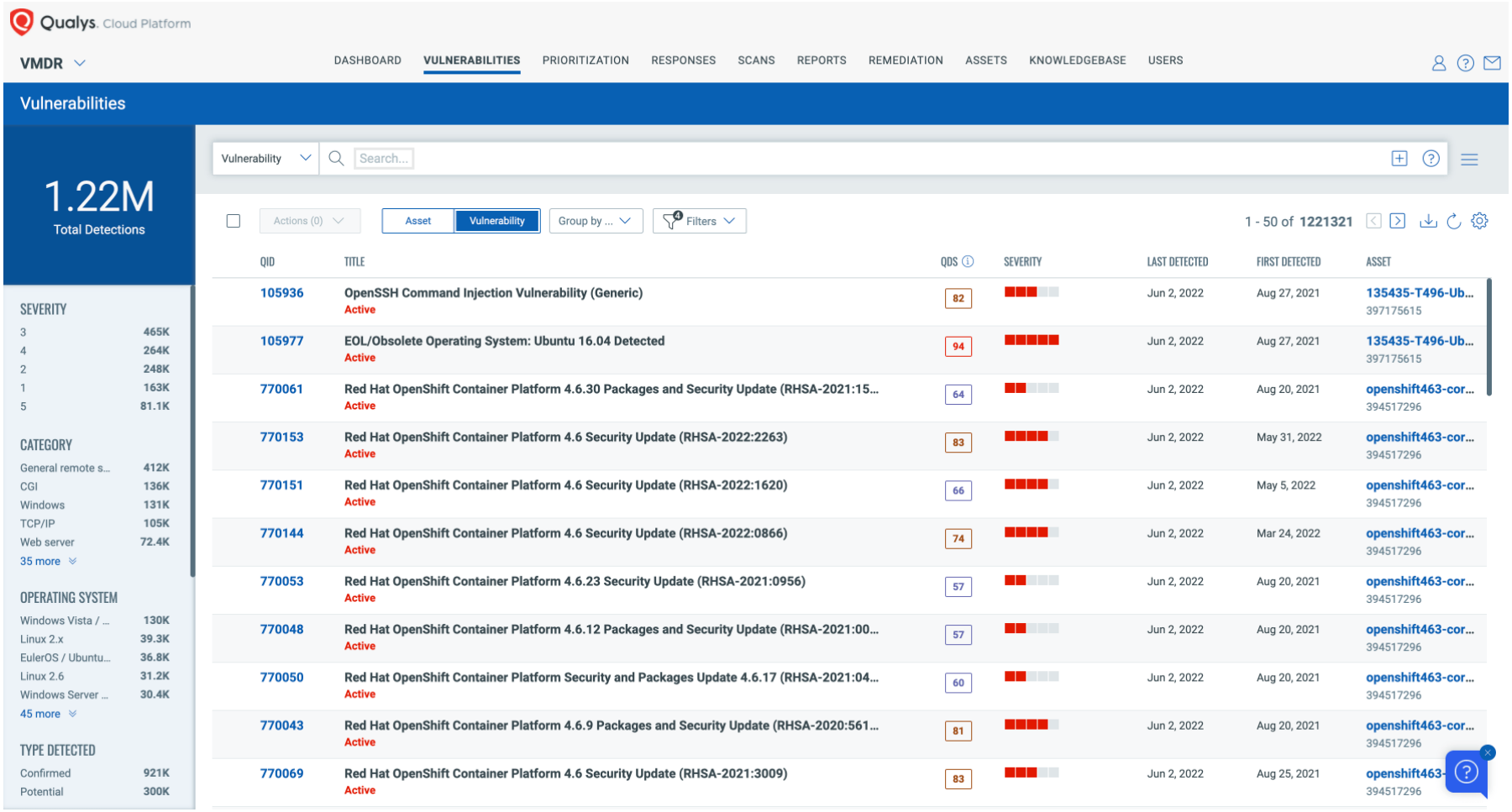
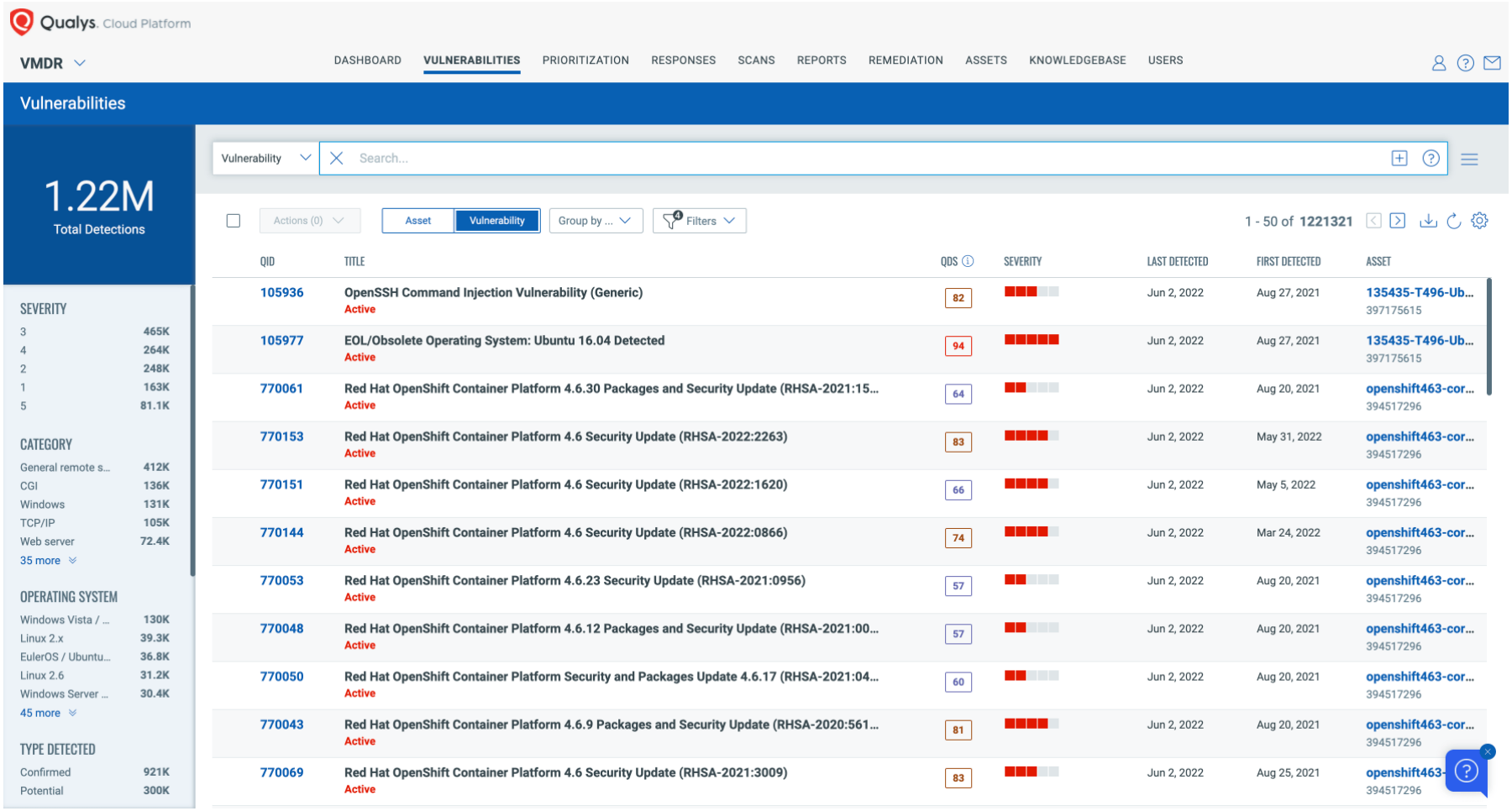
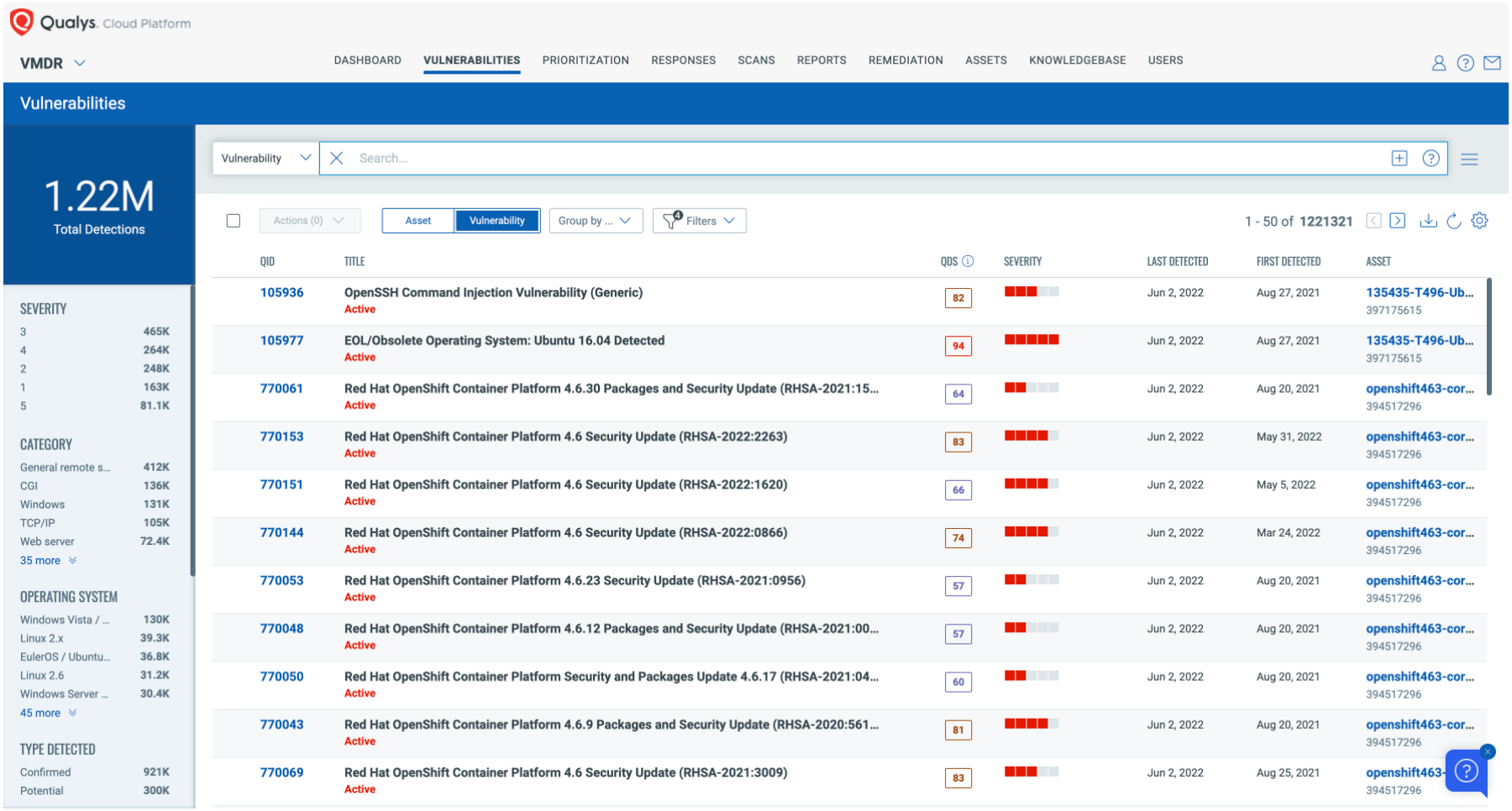
Based on your environment, you can have many vulnerabilities ranging from a few hundred, to millions. It is important to understand the need to prioritize, and which should be remediated first.



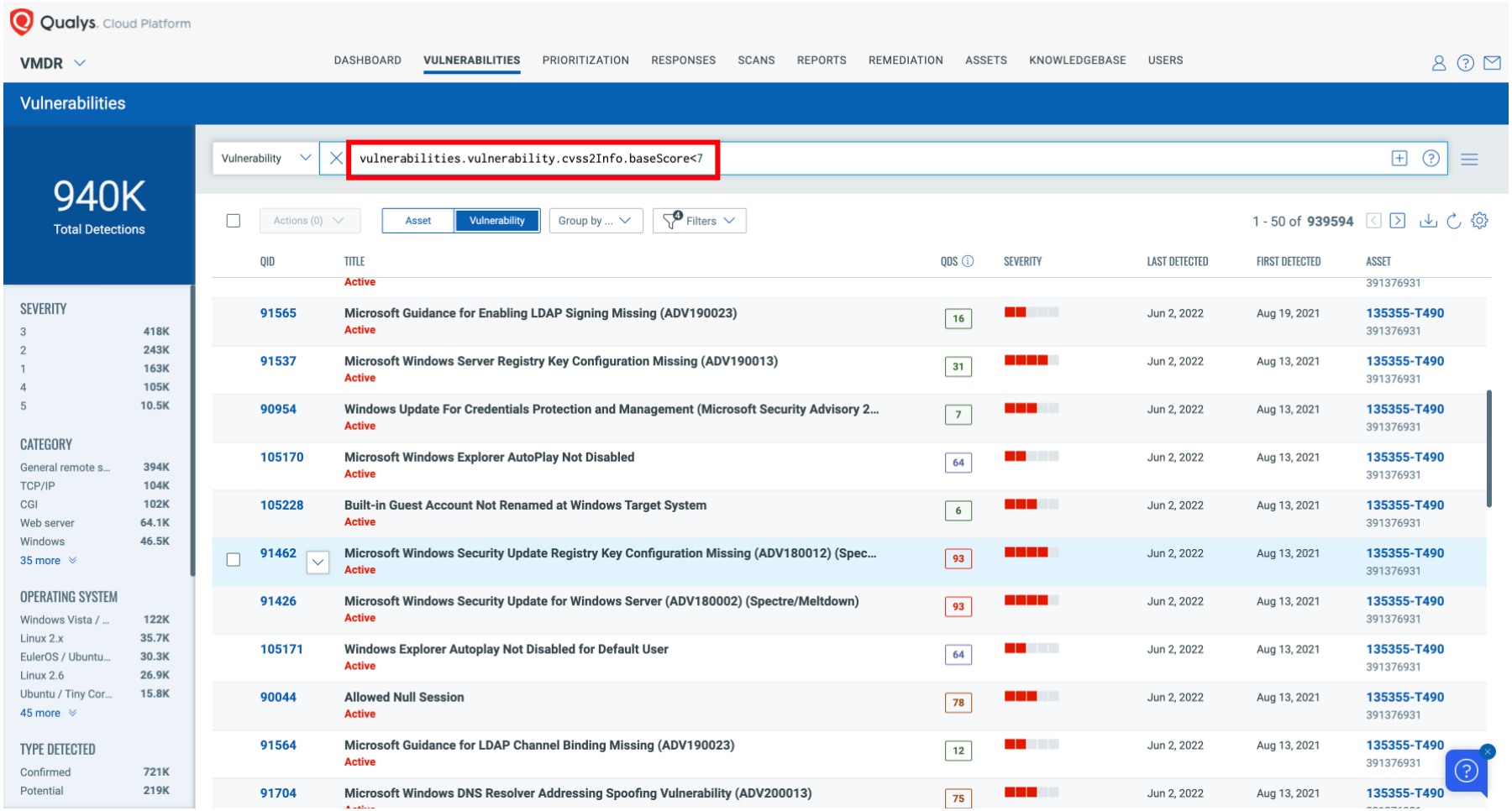
Historically, organizations have relied on CVSS scores. This is only effective to a certain point. A CVSS score does not include external factors like exploit kits or recent exploit trends.



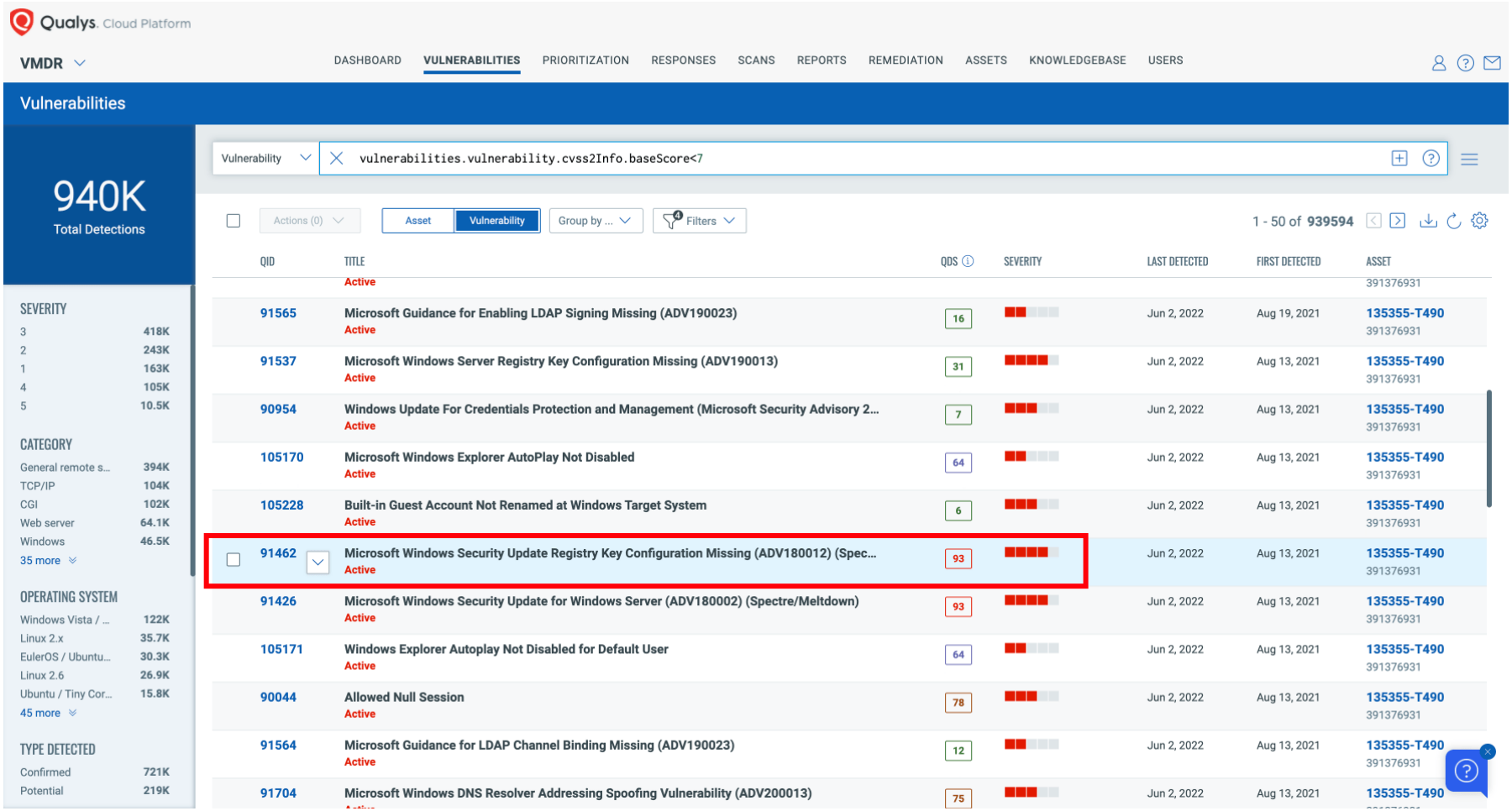
The steps that follow will filter vulnerabilities based on CVSS scores.



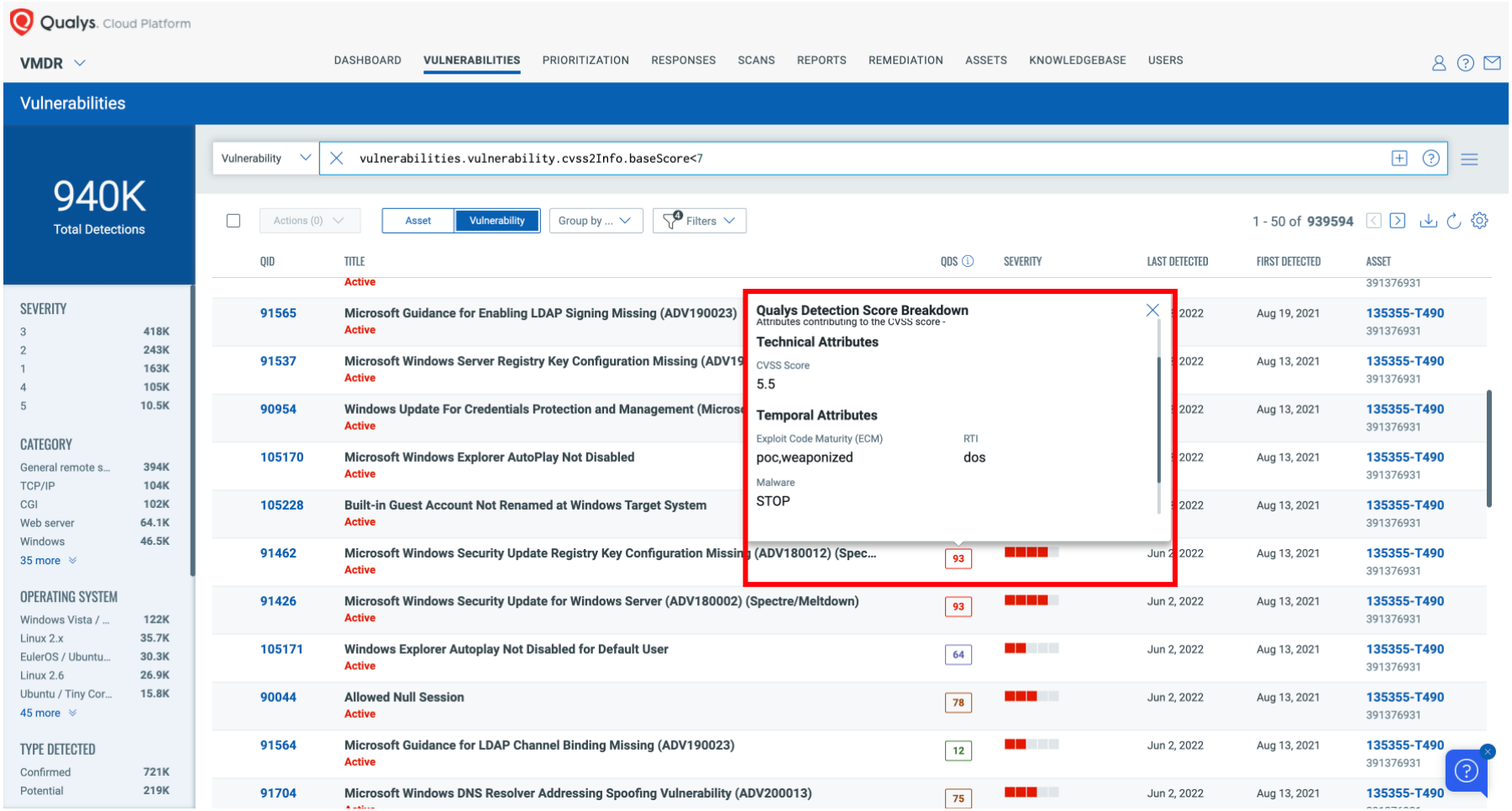
Here we have a query for CVSS base scores less than 7. Only Low to Medium vulnerabilities will be displayed in the dataset.



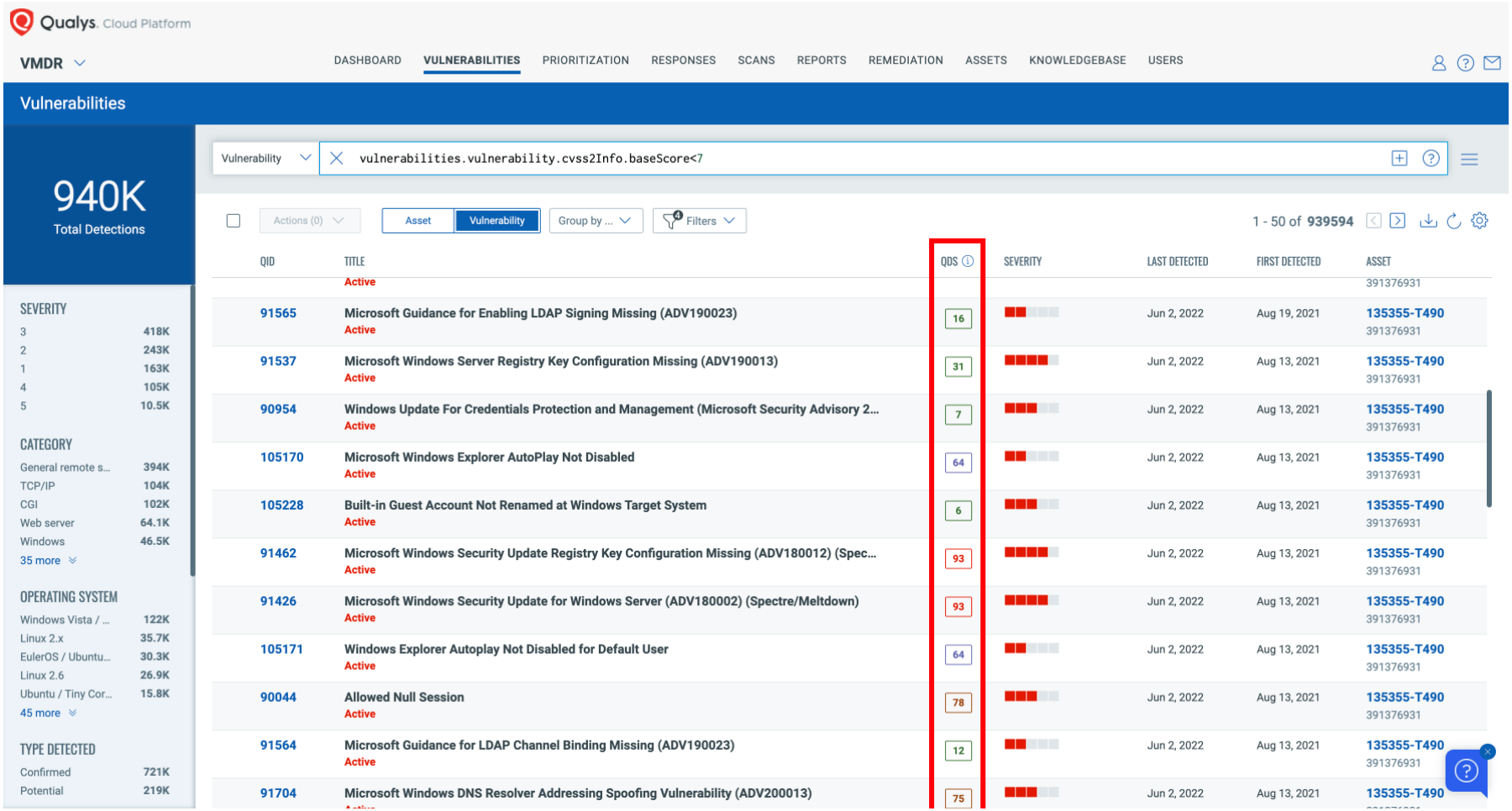
The CVSS base score does not take into account temporal factors, like the availability of exploit code on the dark web.



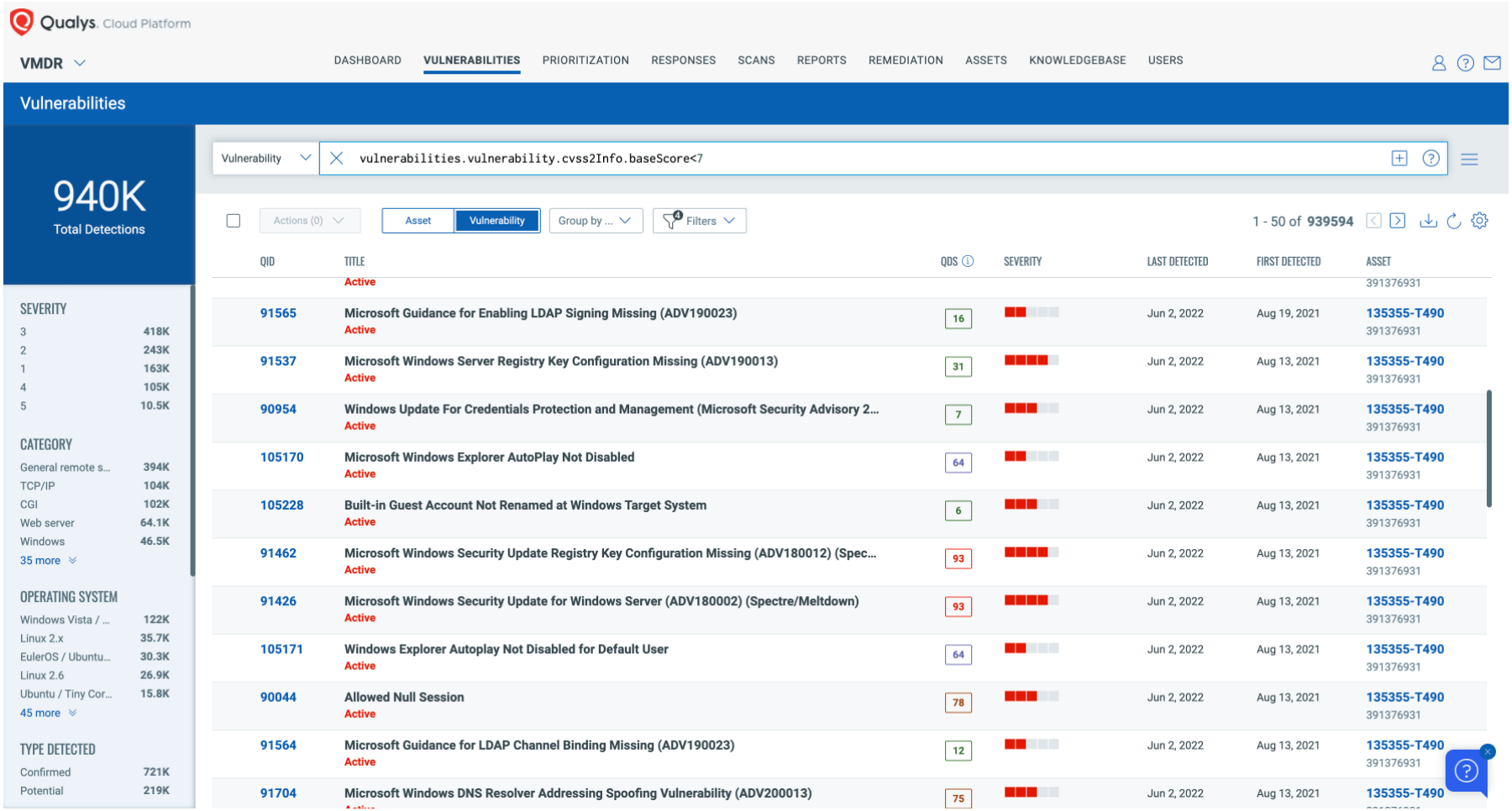
Even though this vulnerability is in the Low to Medium range of CVSS, you can see that the Qualys QDS score is a 93. This is in the critical range of QDS, due to a weaponized exploit kit available.



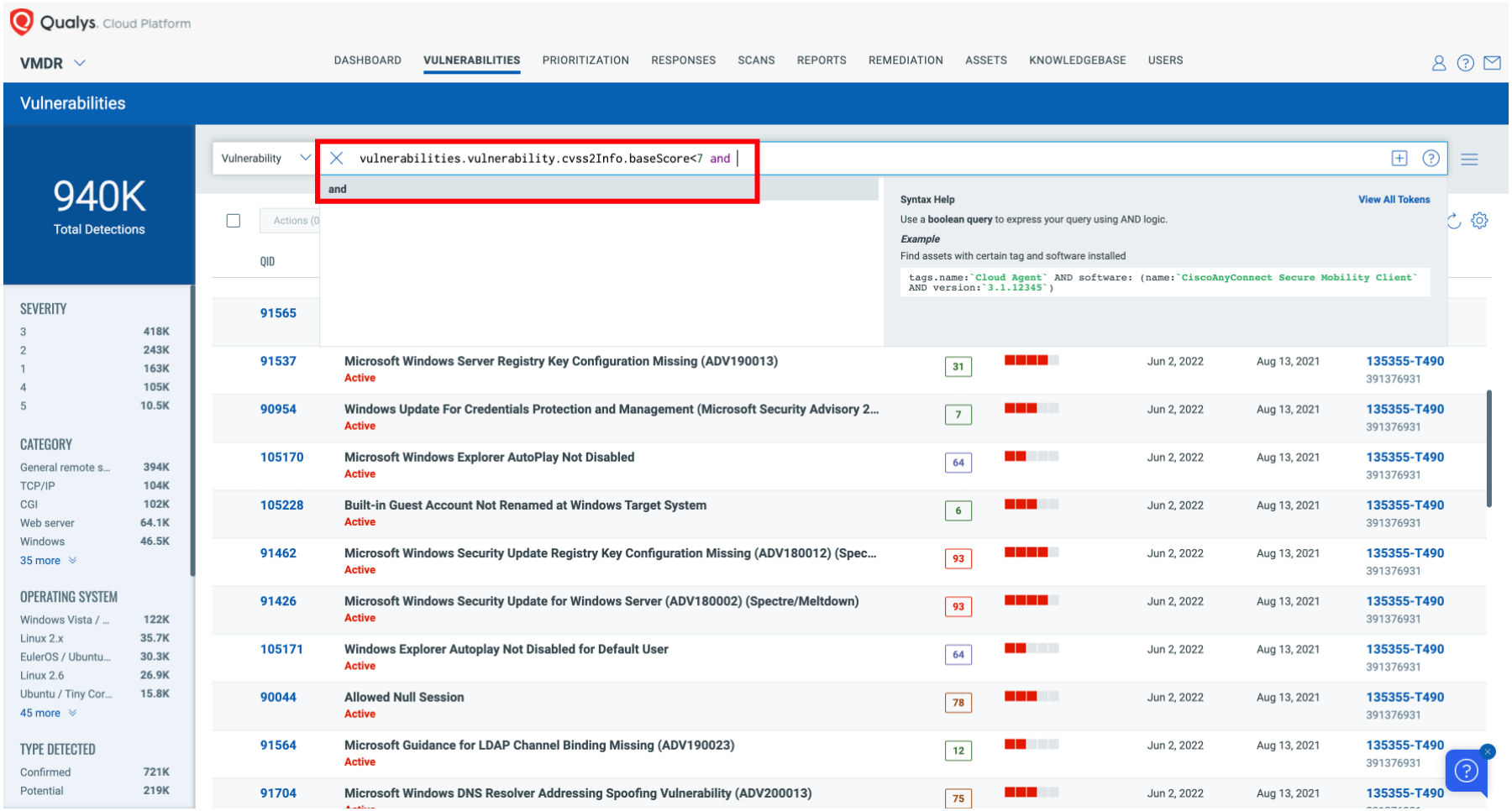
This is why Qualys has developed the Qualys Detection Score. QDS takes CVSS as a key input and adds temporal factors to reflect the risk level of a vulnerability to your organization.



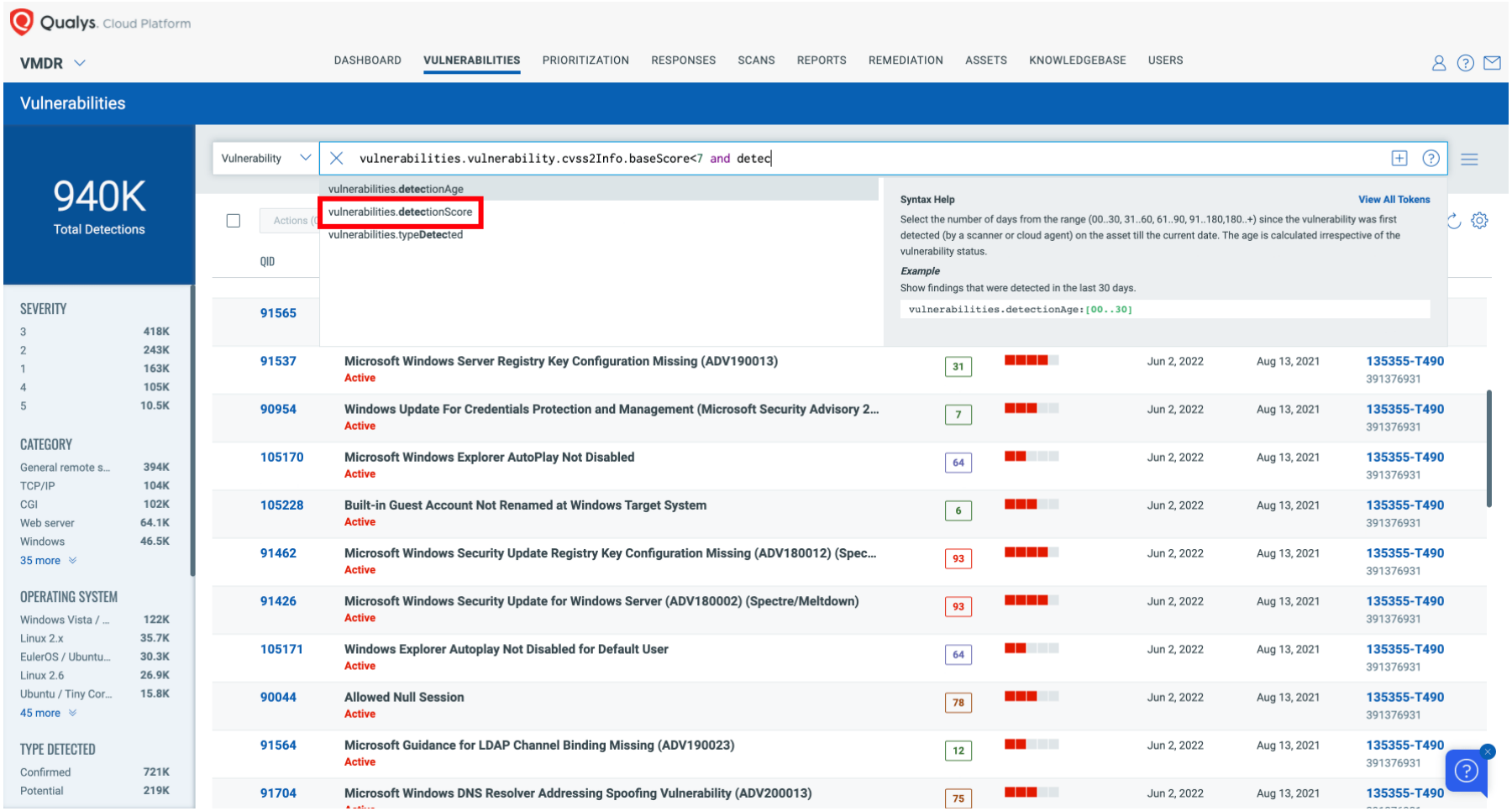
A note here, if mitigation control is applied on a vulnerability, its QDS is reduced.



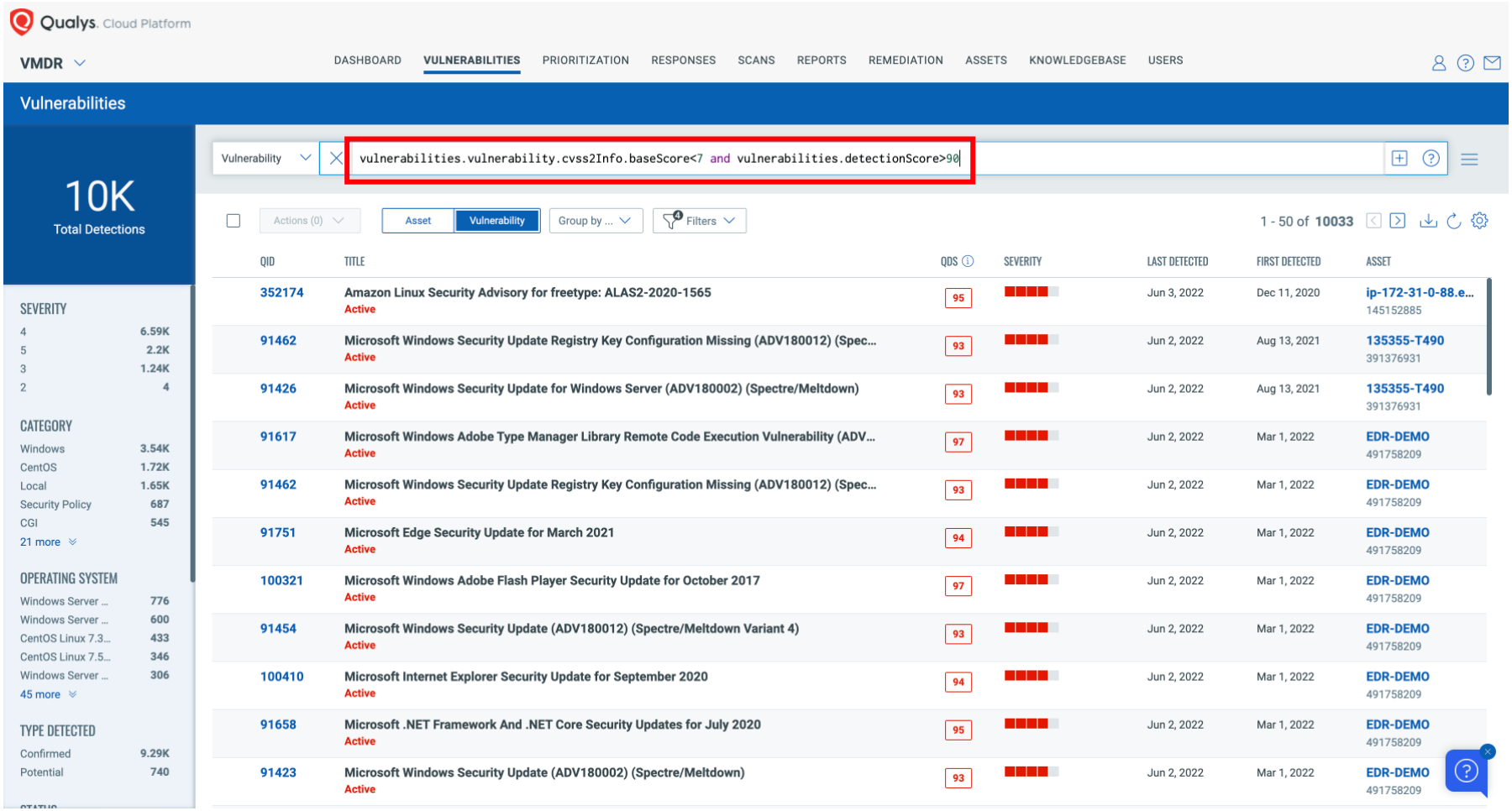
In the steps that follow, the original query will be enhanced to show only Low to Medium CVSS levels that have critical QDS scores.



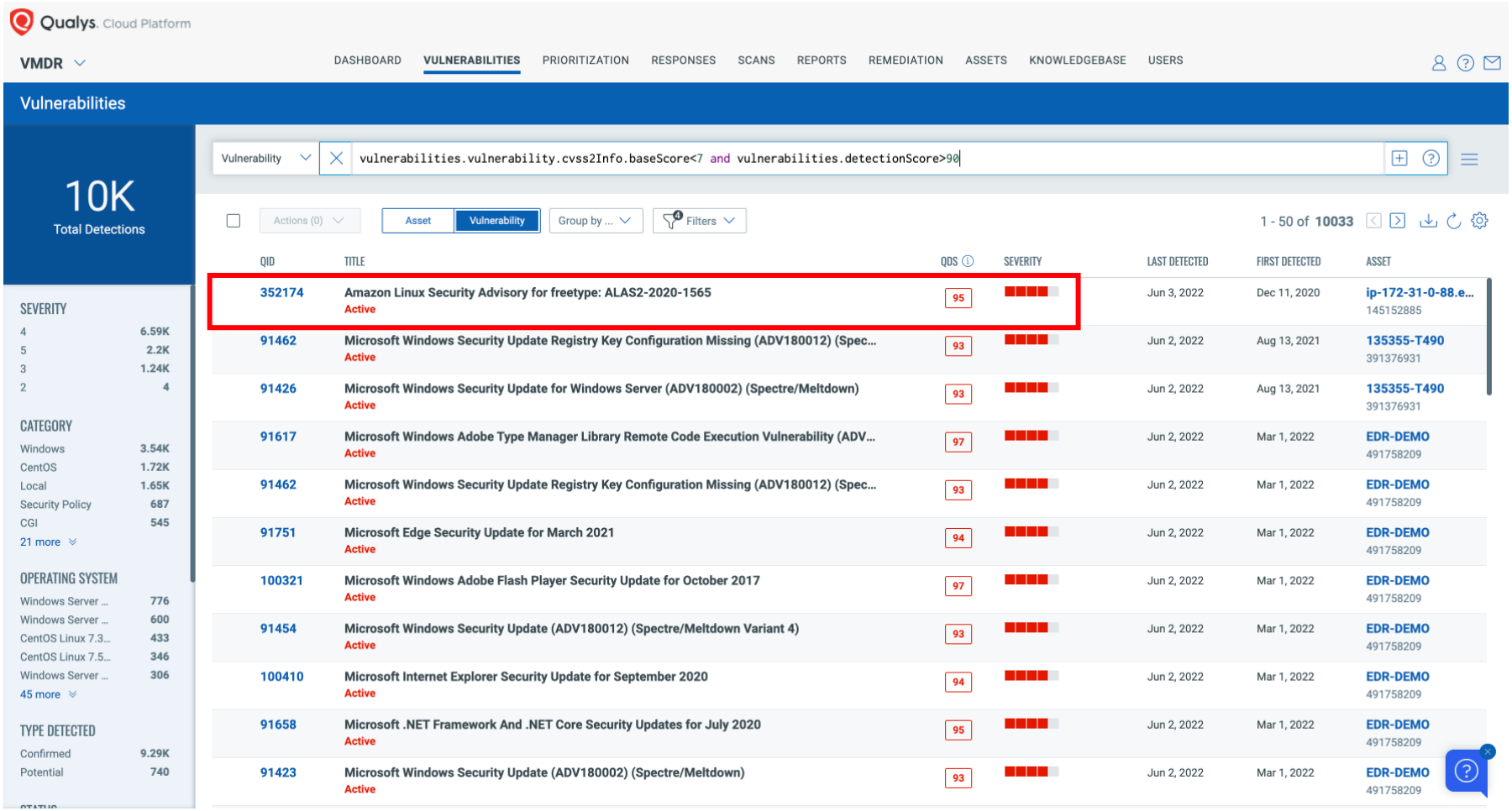
With the interactive help you can see the QDS search token.



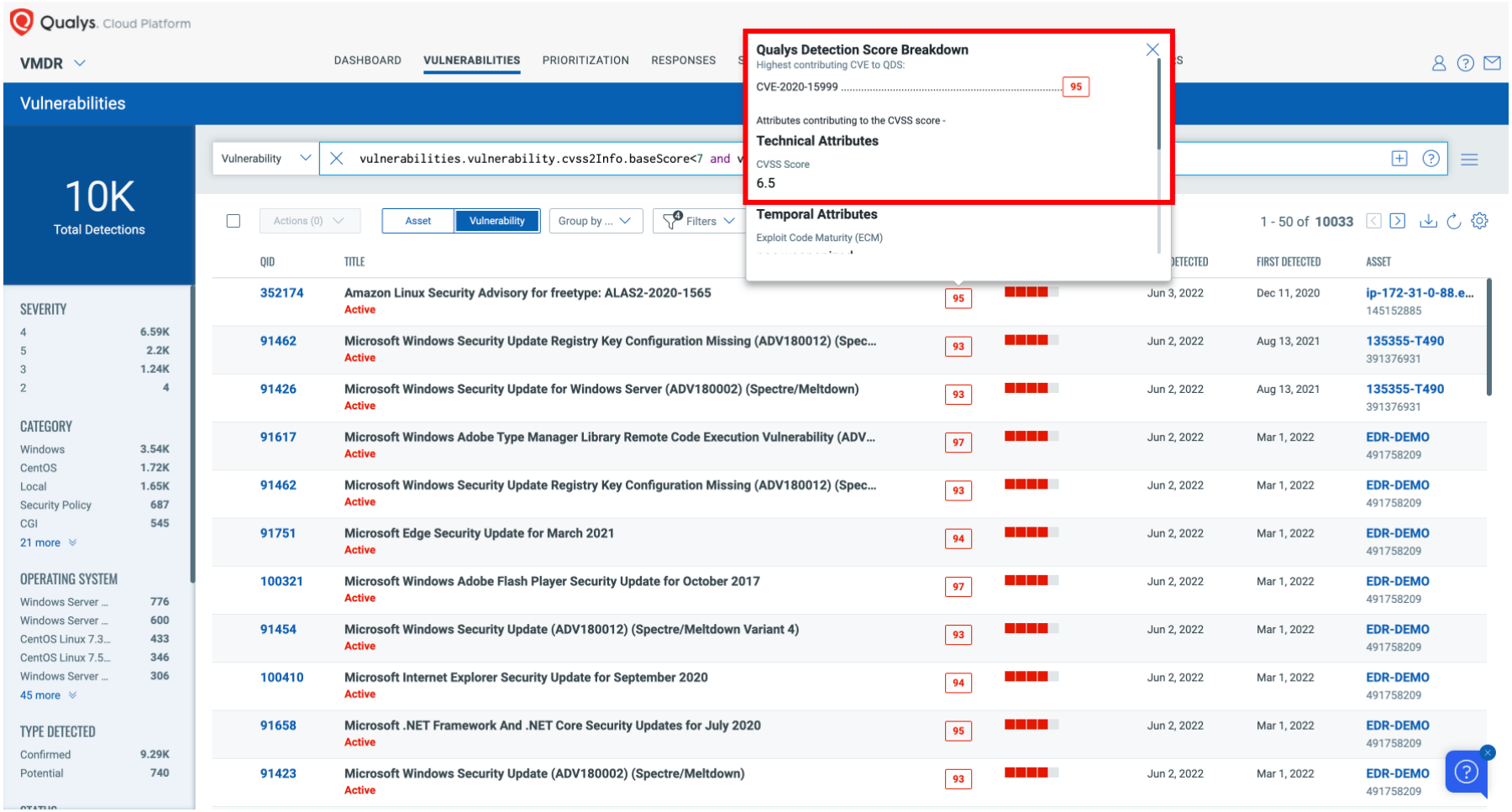
Here you see the full query. The dataset shows vulnerabilities with a Low to Medium CVSS score that pose a critical risk due to different exploitability and trend dynamics.



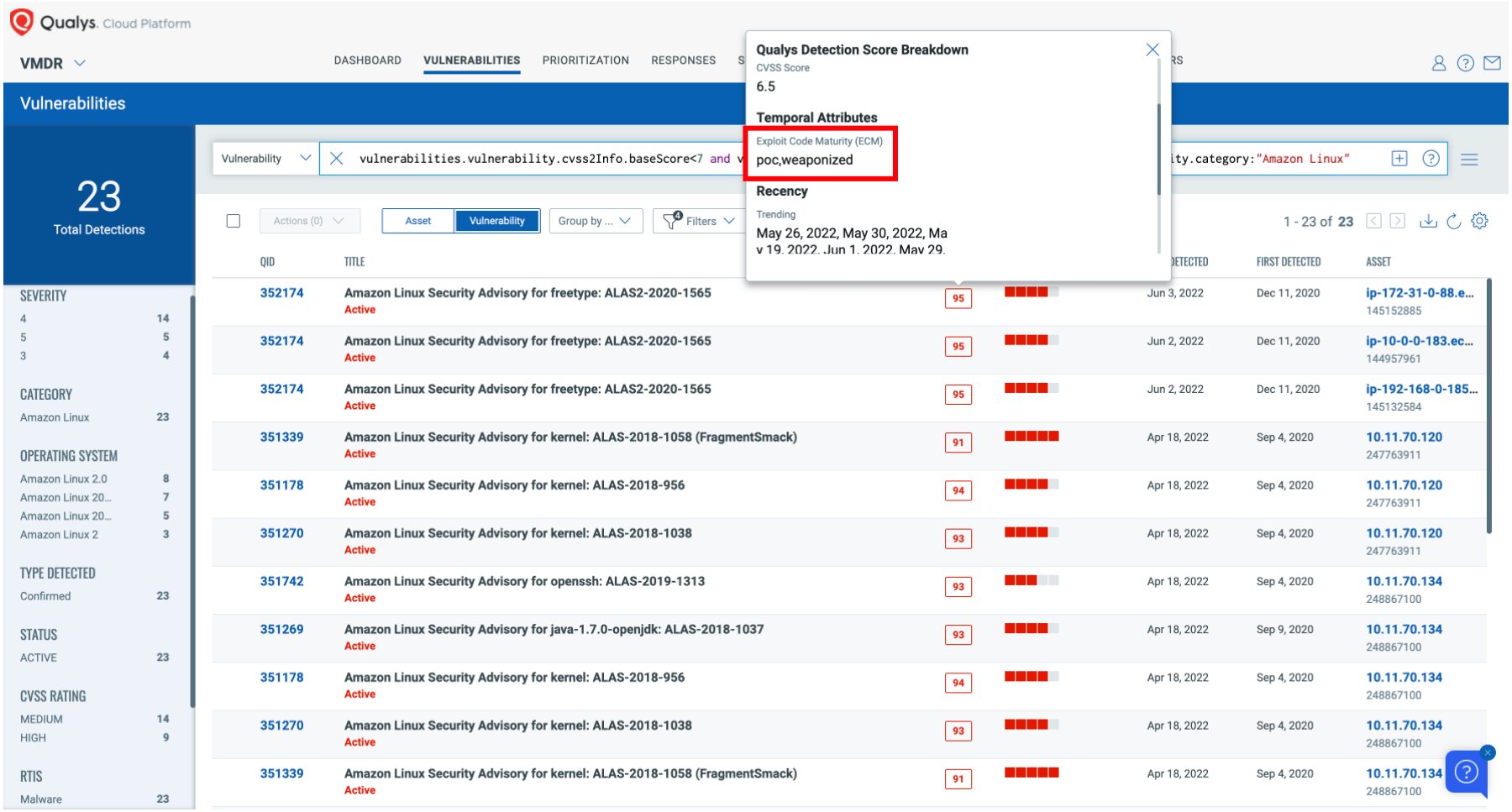
In the steps to follow, you will see the contributing factors of why this highlighted vulnerability has a QDS score of 95.



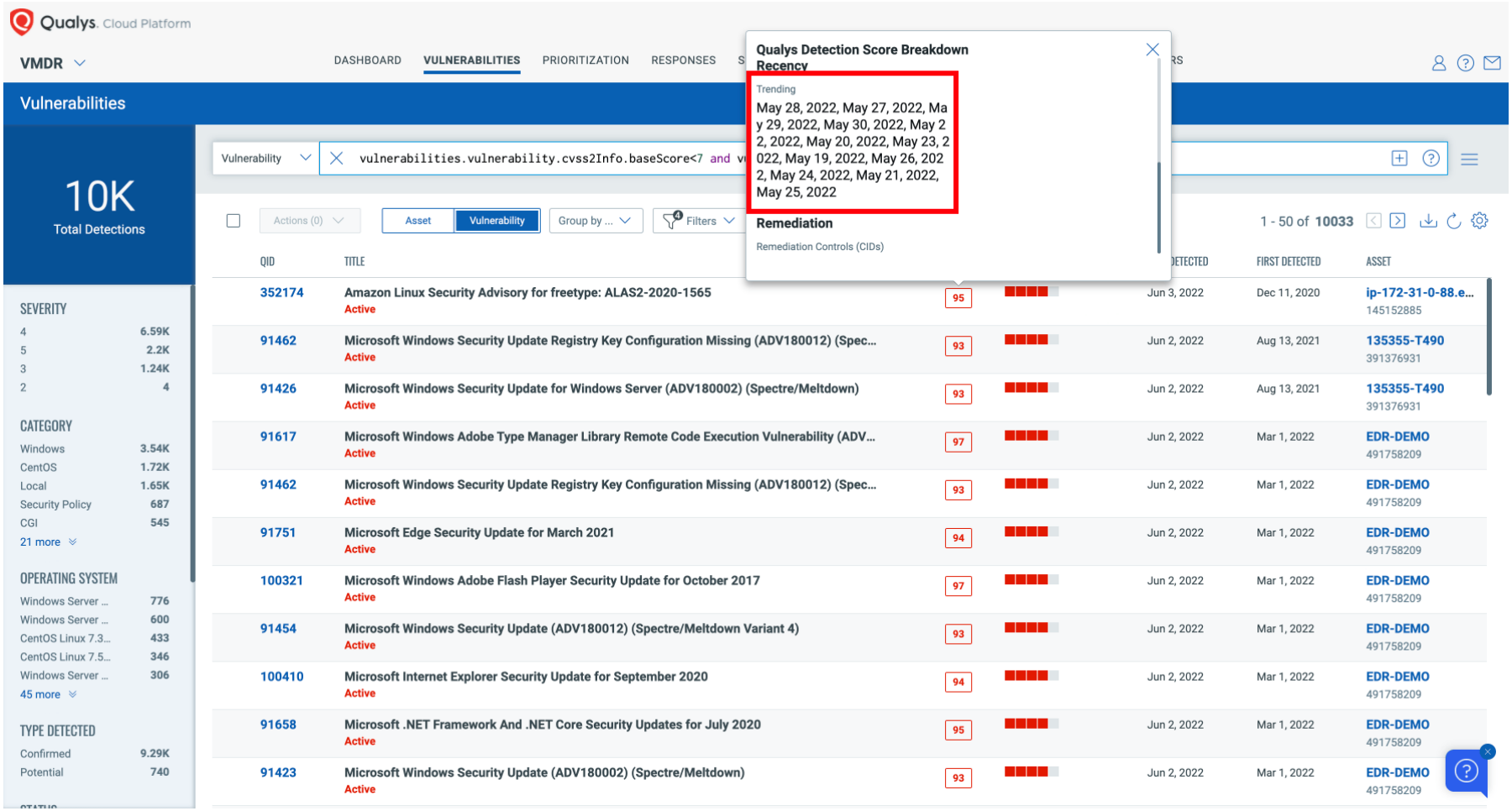
The CVSS score of 6.5 is Medium. The QDS score of 95 is in the critical range of risk. This vulnerability should be prioritized for remediation even though the CVSS score does not reflect the same importance.


Qualys. Cloud Platform
VMDR
DASHBOARD
VULNERABILITIES
PRIORITIZATION
RESPONSES
Vulnerabilities
10K
Total Detections
SEVERITY
4 6.59K
5 2.2K
3 1.24K
2 4
CATEGORY
Windows 3.54K
CentOS 1.72K
Local 1.65K
Security Policy 687
CGI 545
21 more
OPERATING SYSTEM
Windows Server ... 776
Windows Server ... 600
CentOS Linux 7.3... 433
CentOS Linux 7.5... 346
Windows Server ... 306
45 more
TYPE DETECTED
Confirmed 9.29K
Potential 740
Vulnerability
vulnerabilities.vulnerability.cvss2Info.baseScore<7 and
Actions (0)
Asset
Vulnerability
Group by ...
Filters
1 - 50 of 10033
Qualys Detection Score Breakdown
Highest contributing CVE to QDS:
CVE-2020-15999
95
Attributes contributing to the CVSS score -
Technical Attributes
CVSS Score
6.5
Temporal Attributes
Exploit Code Maturity (ECM)
QID
TITLE
FIRST DETECTED
ASSET
352174 Amazon Linux Security Advisory for freetype: ALAS2-2020-1565 Active 95 Jun 3, 2022 Dec 11, 2020 ip-172-31-0-88.e... 145152885
91462 Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spec... Active 93 Jun 2, 2022 Aug 13, 2021 135355-T490 391376931
91426 Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown) Active 93 Jun 2, 2022 Aug 13, 2021 135355-T490 391376931
91617 Microsoft Windows Adobe Type Manager Library Remote Code Execution Vulnerability (ADV... Active 97 Jun 2, 2022 Mar 1, 2022 EDR-DEMO 491758209
91462 Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spec... Active 93 Jun 2, 2022 Mar 1, 2022 EDR-DEMO 491758209
91751 Microsoft Edge Security Update for March 2021 Active 94 Jun 2, 2022 Mar 1, 2022 EDR-DEMO 491758209
100321 Microsoft Windows Adobe Flash Player Security Update for October 2017 Active 97 Jun 2, 2022 Mar 1, 2022 EDR-DEMO 491758209
91454 Microsoft Windows Security Update (ADV180012) (Spectre/Meltdown Variant 4) Active 93 Jun 2, 2022 Mar 1, 2022 EDR-DEMO 491758209
100410 Microsoft Internet Explorer Security Update for September 2020 Active 94 Jun 2, 2022 Mar 1, 2022 EDR-DEMO 491758209
91658 Microsoft .NET Framework And .NET Core Security Updates for July 2020 Active 95 Jun 2, 2022 Mar 1, 2022 EDR-DEMO 491758209
91423 Microsoft Windows Security Update (ADV180002) (Spectre/Meltdown) Active 93 Jun 2, 2022 Mar 1, 2022 EDR-DEMO 491758209

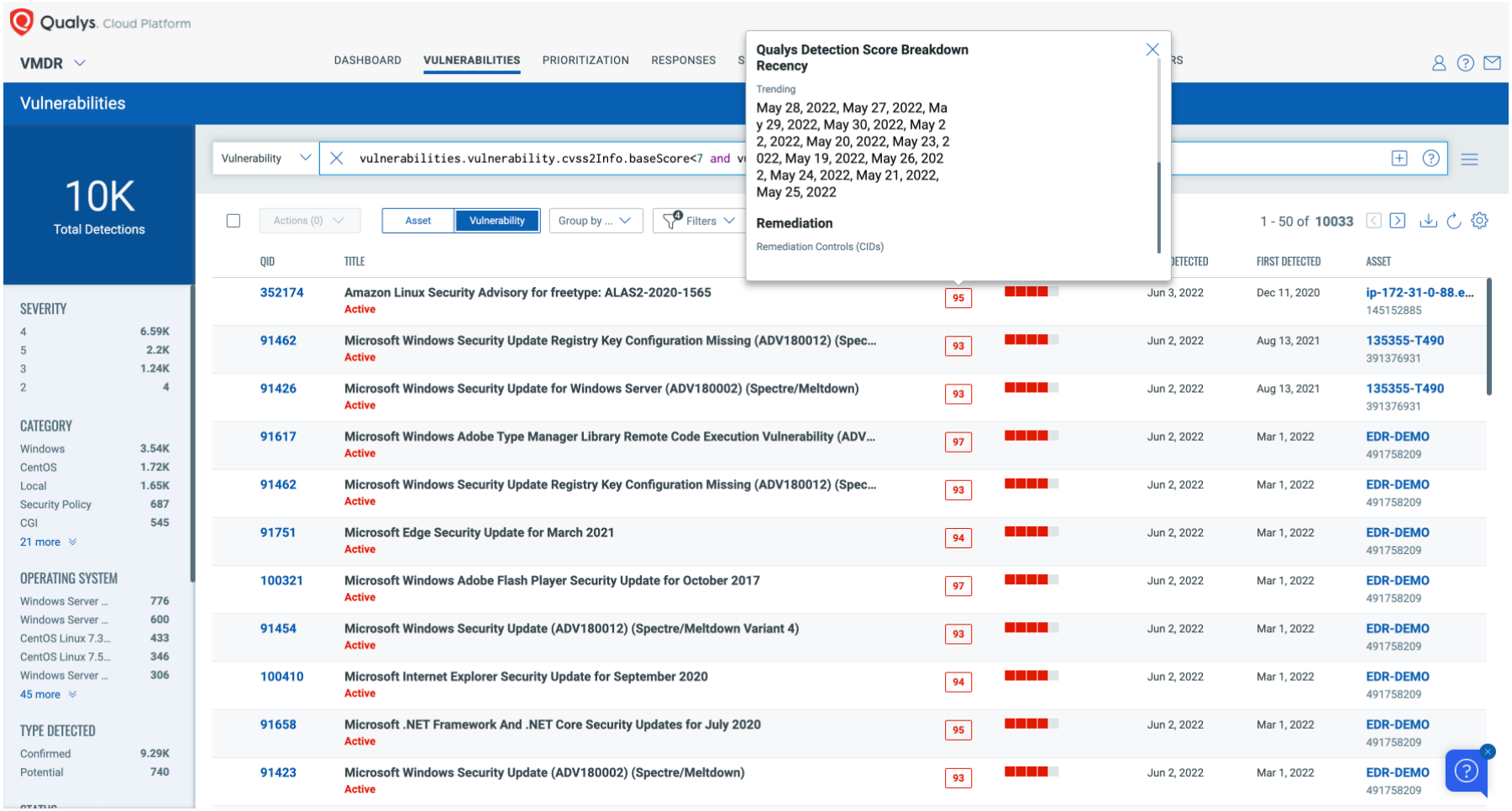
Under Exploit Code Maturity, proof of concept means that the vulnerability is a threat, but not that potent. Once it is weaponized, the attacker can easily exploit the system. Here you see both poc and weaponized are listed.


Qualys. Cloud Platform
VMDR
DASHBOARD
VULNERABILITIES
PRIORITIZATION
RESPONSES
Vulnerabilities
23
Total Detections
SEVERITY
4 14
5 5
3 4
CATEGORY
Amazon Linux 23
OPERATING SYSTEM
Amazon Linux 2.0 8
Amazon Linux 20... 7
Amazon Linux 20... 5
Amazon Linux 2 3
TYPE DETECTED
Confirmed 23
STATUS
ACTIVE 23
CVSS RATING
MEDIUM 14
HIGH 9
RTIS
Malware 23
Vulnerability
vulnerabilities.vulnerability.cvss2Info.baseScore<7 and
ity.category:"Amazon Linux"
Actions (0)
Asset
Vulnerability
Group by ...
Filters
1 - 23 of 23
Qualys Detection Score Breakdown
CVSS Score
6.5
Temporal Attributes
Exploit Code Maturity (ECM)
poc,weaponized
Recency
Trending
May 26, 2022, May 30, 2022, Ma
v 19, 2022, Jun 1, 2022, May 29,
QID
TITLE
DETECTED
FIRST DETECTED
ASSET
352174 Amazon Linux Security Advisory for freetype: ALAS2-2020-1565 Active 95 Jun 3, 2022 Dec 11, 2020 ip-172-31-0-88.e... 145152885
352174 Amazon Linux Security Advisory for freetype: ALAS2-2020-1565 Active 95 Jun 2, 2022 Dec 11, 2020 ip-10-0-0-183.ec... 144957961
352174 Amazon Linux Security Advisory for freetype: ALAS2-2020-1565 Active 95 Jun 2, 2022 Dec 11, 2020 ip-192-168-0-185... 145132584
351339 Amazon Linux Security Advisory for kernel: ALAS-2018-1058 (FragmentSmack) Active 91 Apr 18, 2022 Sep 4, 2020 10.11.70.120 247763911
351178 Amazon Linux Security Advisory for kernel: ALAS-2018-956 Active 94 Apr 18, 2022 Sep 4, 2020 10.11.70.120 247763911
351270 Amazon Linux Security Advisory for kernel: ALAS-2018-1038 Active 93 Apr 18, 2022 Sep 4, 2020 10.11.70.120 247763911
351742 Amazon Linux Security Advisory for openssh: ALAS-2019-1313 Active 93 Apr 18, 2022 Sep 4, 2020 10.11.70.134 248867100
351269 Amazon Linux Security Advisory for java-1.7.0-openjdk: ALAS-2018-1037 Active 93 Apr 18, 2022 Sep 9, 2020 10.11.70.134 248867100
351178 Amazon Linux Security Advisory for kernel: ALAS-2018-956 Active 94 Apr 18, 2022 Sep 4, 2020 10.11.70.134 248867100
351270 Amazon Linux Security Advisory for kernel: ALAS-2018-1038 Active 93 Apr 18, 2022 Sep 4, 2020 10.11.70.134 248867100
351339 Amazon Linux Security Advisory for kernel: ALAS-2018-1058 (FragmentSmack) Active 91 Apr 18, 2022 Sep 4, 2020 10.11.70.134 248867100

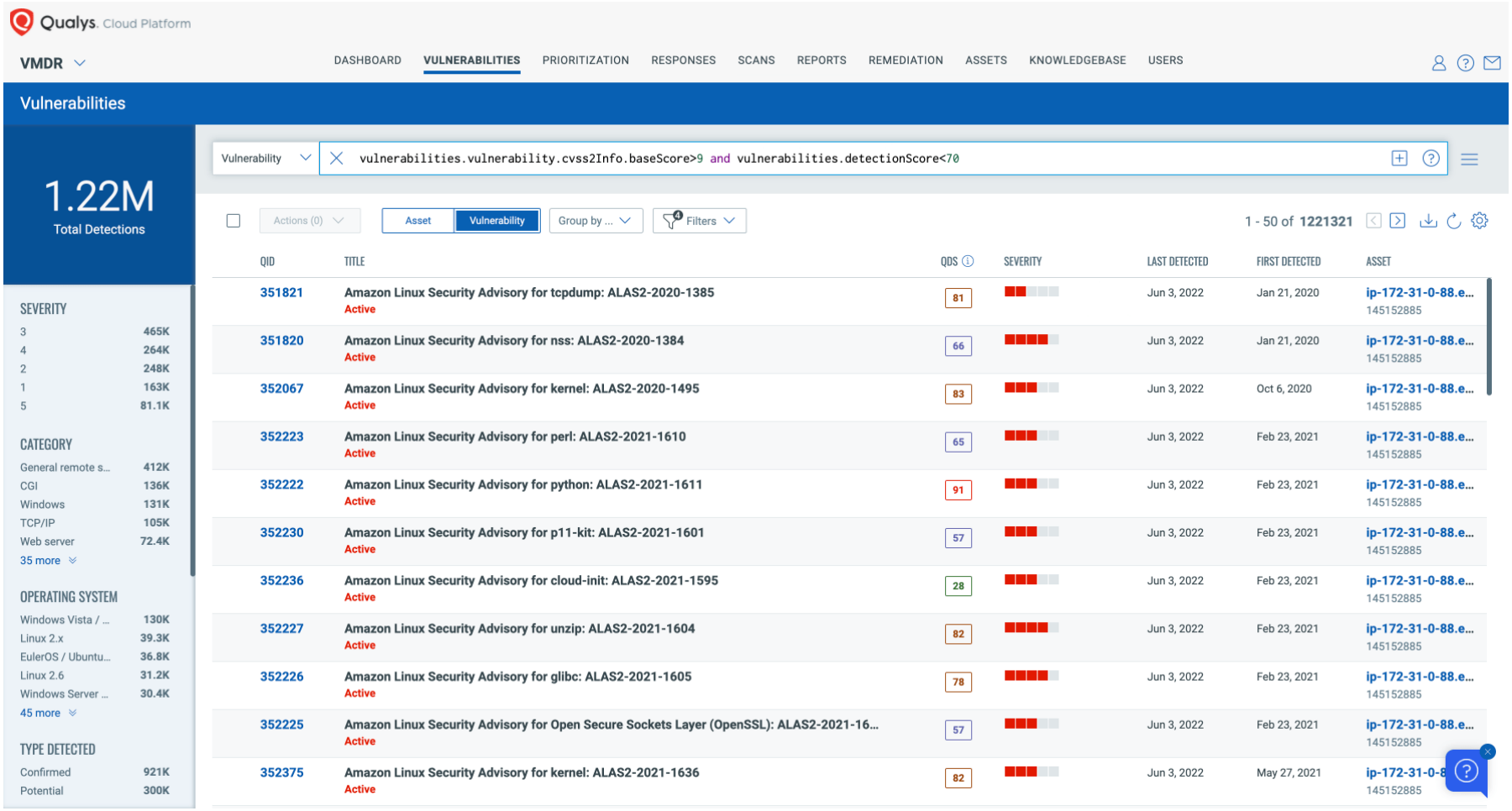
Here you can see that the vulnerability has been recently trending on social media and the dark web.



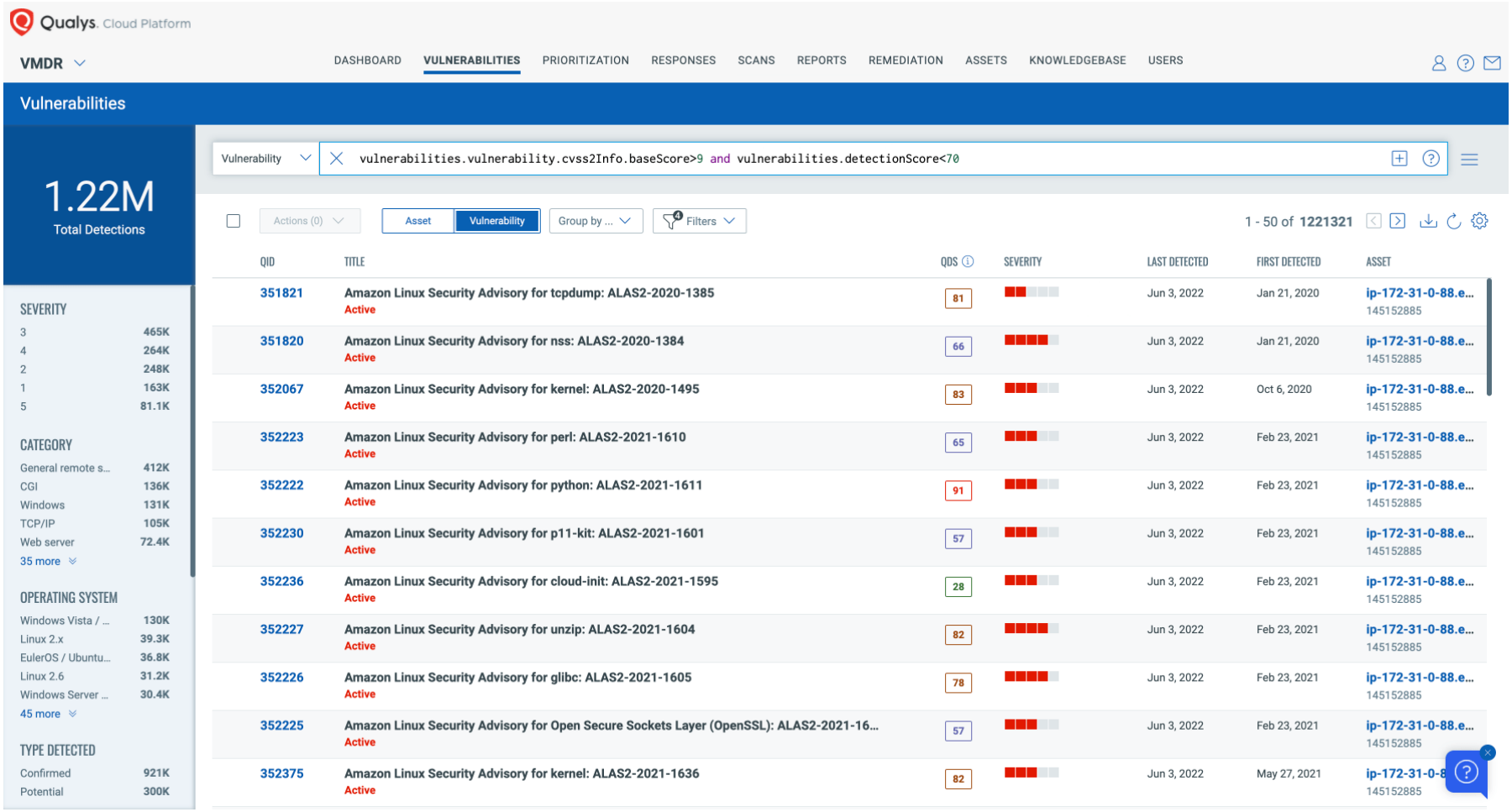
The exploit and trend dynamics of this Amazon Linux vulnerability reflect a high risk even though the CVSS score is in the Medium range.



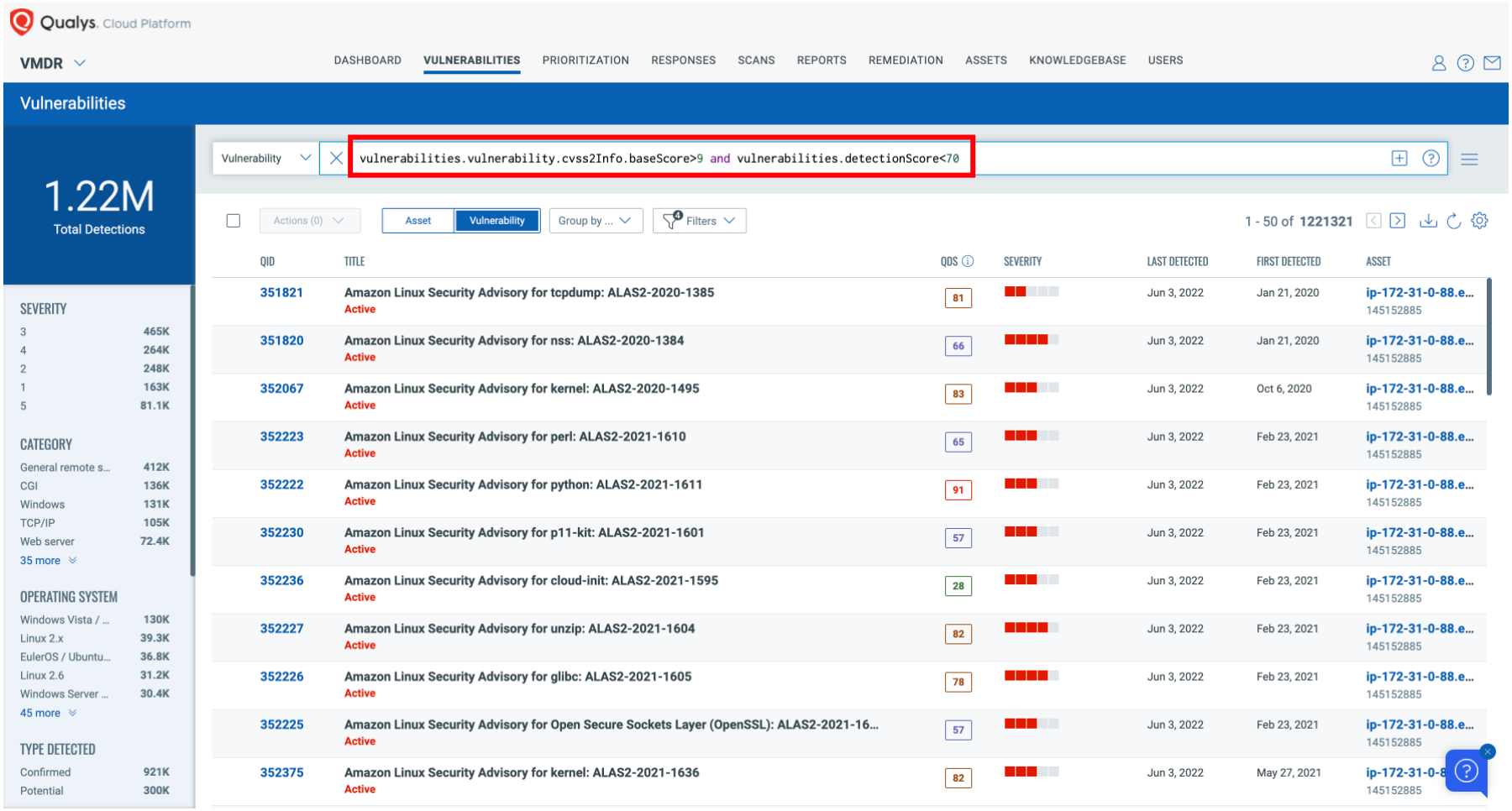
The steps that follow will address an alternate example. A vulnerability can have a high CVSS score, but not pose the same level of risk.



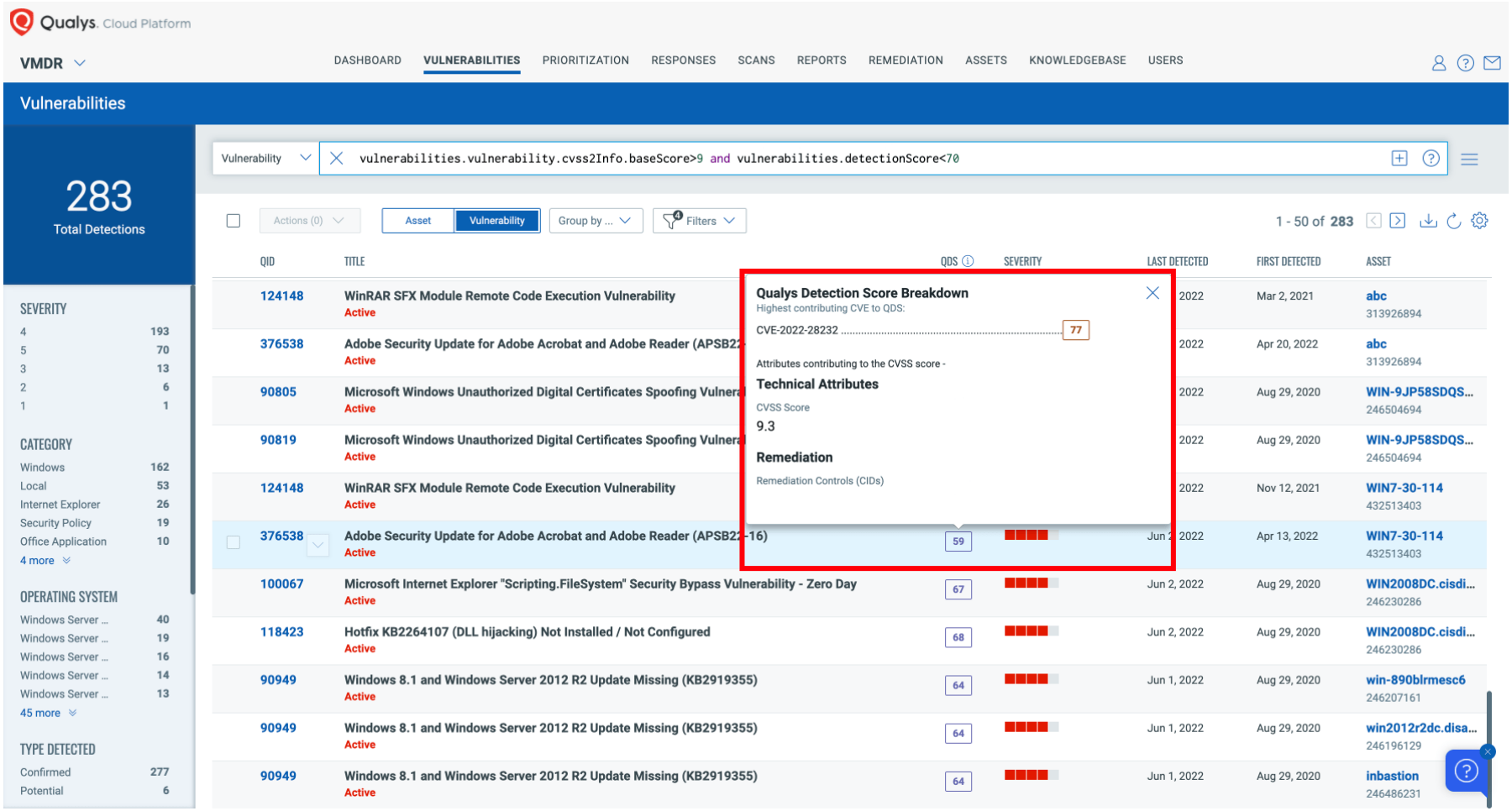
This could be due to an absence of exploits. In this case, you would prioritize remediation lower, in favor of more risky vulnerabilities to your organization. This way, your remediation resources are maximizing their efficiency.


Qualys. Cloud Platform
VMDR
DASHBOARD
VULNERABILITIES
PRIORITIZATION
RESPONSES
SCANS
REPORTS
REMEDIATION
ASSETS
KNOWLEDGEBASE
USERS
Vulnerabilities
1.22M
Total Detections
Vulnerability
vulnerabilities.vulnerability.cvss2Info.baseScore>9 and vulnerabilities.detectionScore<70
Actions (0)
Asset
Vulnerability
Group by ...
Filters
1 - 50 of 1221321
SEVERITY
3 465K
4 264K
2 248K
1 163K
5 81.1K
CATEGORY
General remote s... 412K
CGI 136K
Windows 131K
TCP/IP 105K
Web server 72.4K
35 more
OPERATING SYSTEM
Windows Vista / ... 130K
Linux 2.x 39.3K
EulerOS / Ubuntu... 36.8K
Linux 2.6 31.2K
Windows Server ... 30.4K
45 more
TYPE DETECTED
Confirmed 921K
Potential 300K
QID
TITLE
QDS
SEVERITY
LAST DETECTED
FIRST DETECTED
ASSET
351821 Amazon Linux Security Advisory for tcpdump: ALAS2-2020-1385 Active 81 Jun 3, 2022 Jan 21, 2020 ip-172-31-0-88.e... 145152885
351820 Amazon Linux Security Advisory for nss: ALAS2-2020-1384 Active 66 Jun 3, 2022 Jan 21, 2020 ip-172-31-0-88.e... 145152885
352067 Amazon Linux Security Advisory for kernel: ALAS2-2020-1495 Active 83 Jun 3, 2022 Oct 6, 2020 ip-172-31-0-88.e... 145152885
352223 Amazon Linux Security Advisory for perl: ALAS2-2021-1610 Active 65 Jun 3, 2022 Feb 23, 2021 ip-172-31-0-88.e... 145152885
352222 Amazon Linux Security Advisory for python: ALAS2-2021-1611 Active 91 Jun 3, 2022 Feb 23, 2021 ip-172-31-0-88.e... 145152885
352230 Amazon Linux Security Advisory for p11-kit: ALAS2-2021-1601 Active 57 Jun 3, 2022 Feb 23, 2021 ip-172-31-0-88.e... 145152885
352236 Amazon Linux Security Advisory for cloud-init: ALAS2-2021-1595 Active 28 Jun 3, 2022 Feb 23, 2021 ip-172-31-0-88.e... 145152885
352227 Amazon Linux Security Advisory for unzip: ALAS2-2021-1604 Active 82 Jun 3, 2022 Feb 23, 2021 ip-172-31-0-88.e... 145152885
352226 Amazon Linux Security Advisory for glibc: ALAS2-2021-1605 Active 78 Jun 3, 2022 Feb 23, 2021 ip-172-31-0-88.e... 145152885
352225 Amazon Linux Security Advisory for Open Secure Sockets Layer (OpenSSL): ALAS2-2021-16... Active 57 Jun 3, 2022 Feb 23, 2021 ip-172-31-0-88.e... 145152885
352375 Amazon Linux Security Advisory for kernel: ALAS2-2021-1636 Active 82 Jun 3, 2022 May 27, 2021 ip-172-31-0-8 145152885

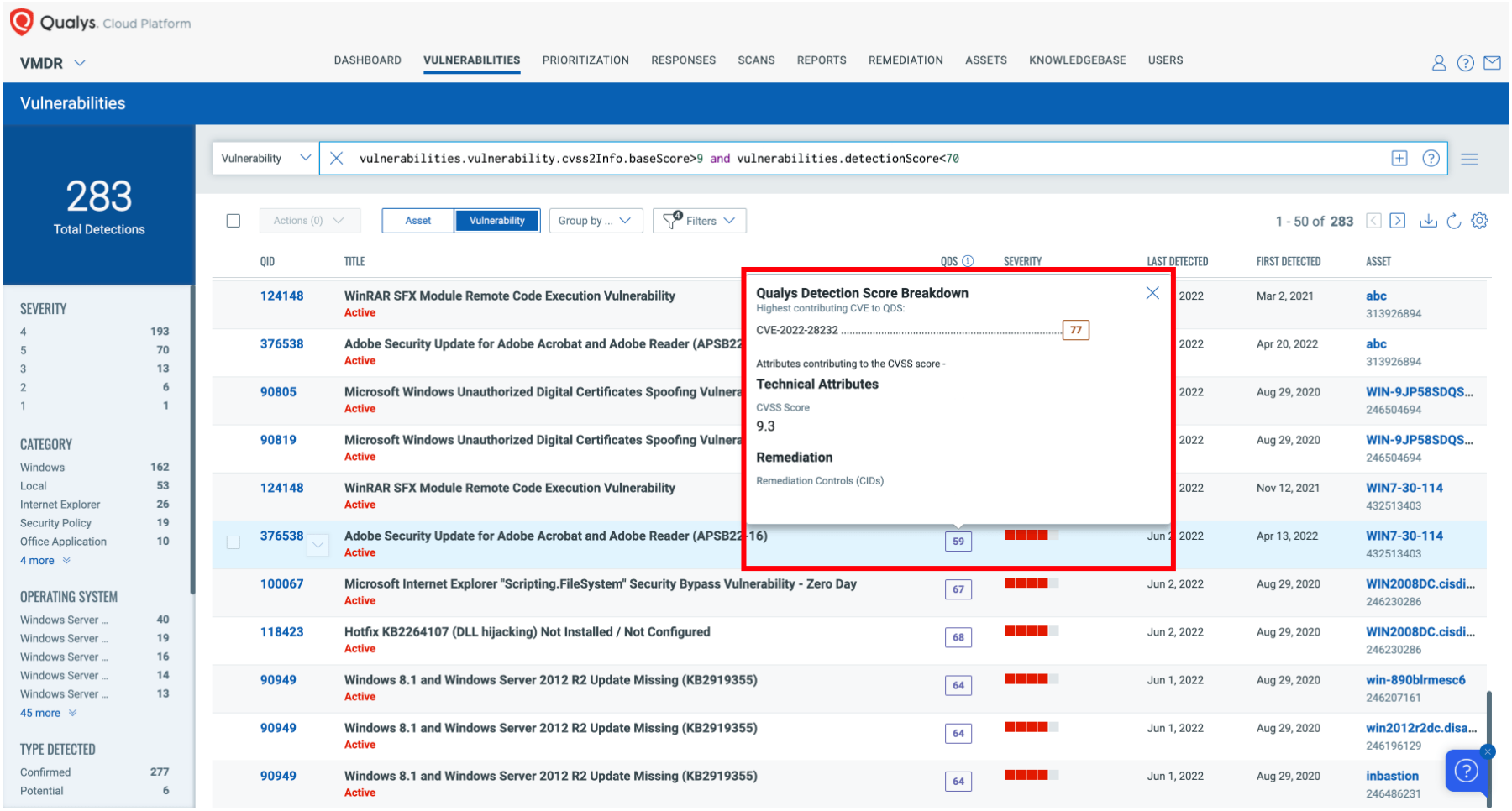
The highlighted query shows a dataset of Critical level CVSS base scores and QDS scores in the Medium to Low range of risk.



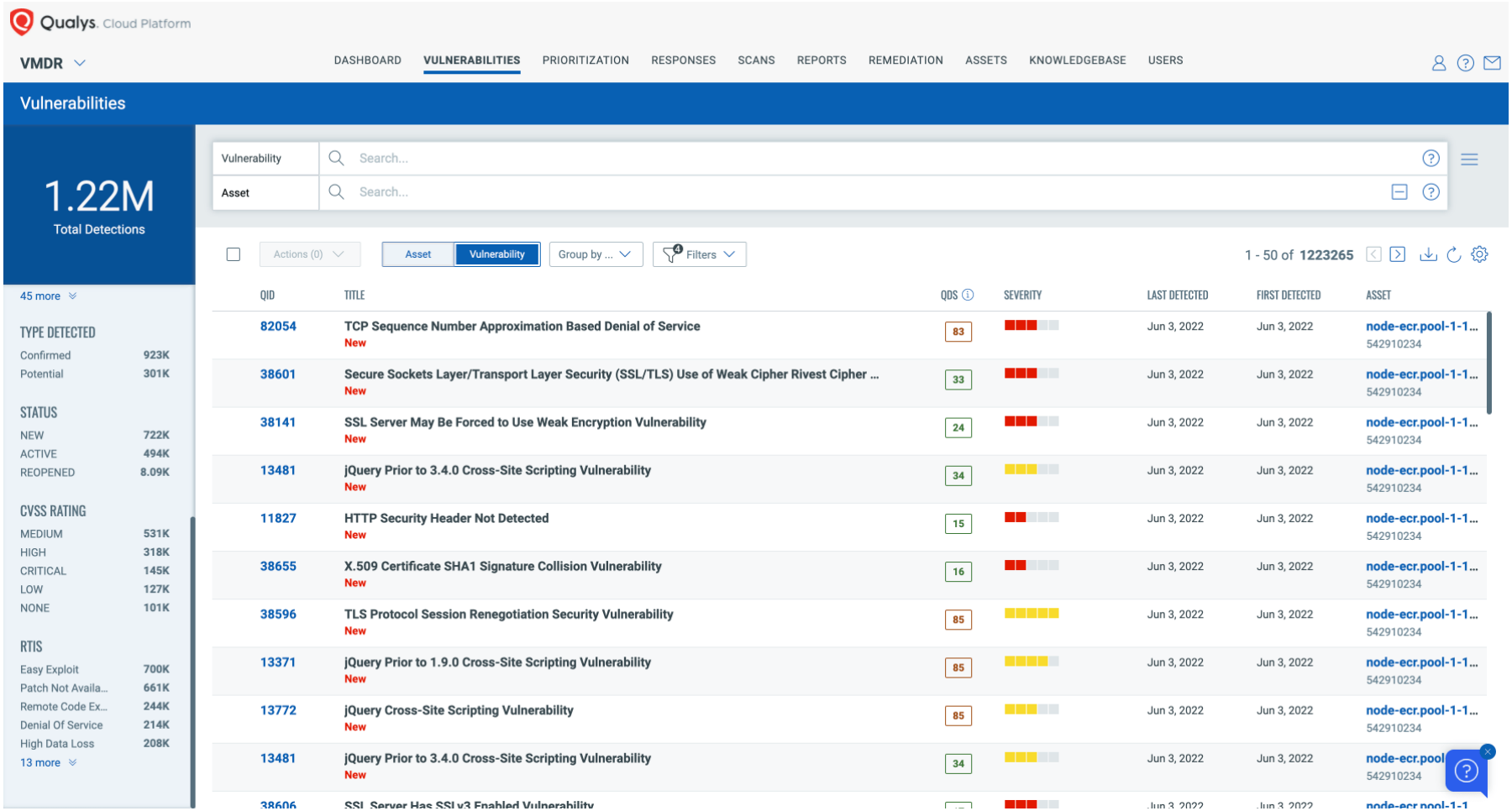
This vulnerability has a very high CVSS score; however, the QDS score does not reflect the same importance.



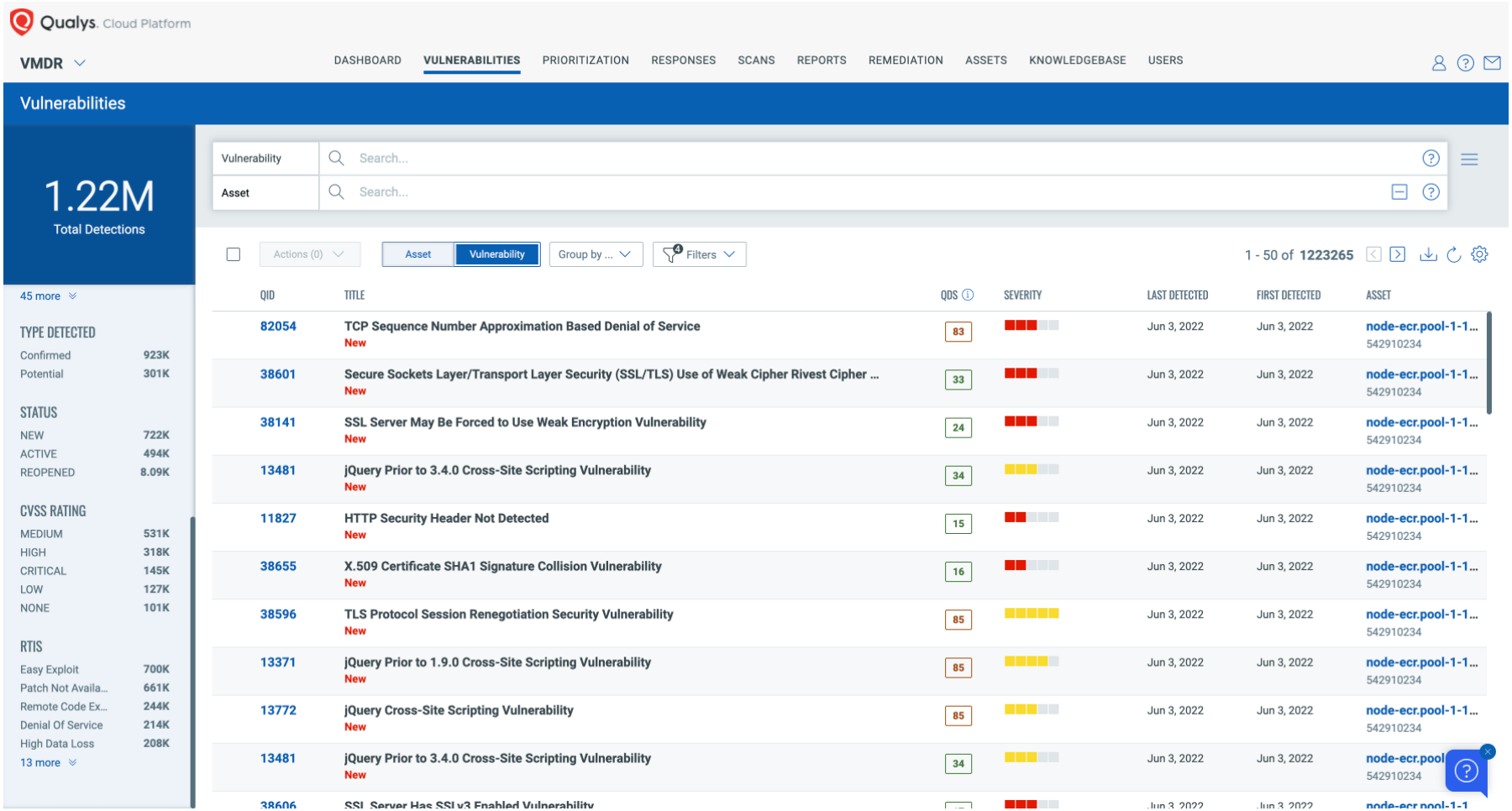
The lower QDS reflects that there is no evidence of exploit kits or imminent attacks for this vulnerability.



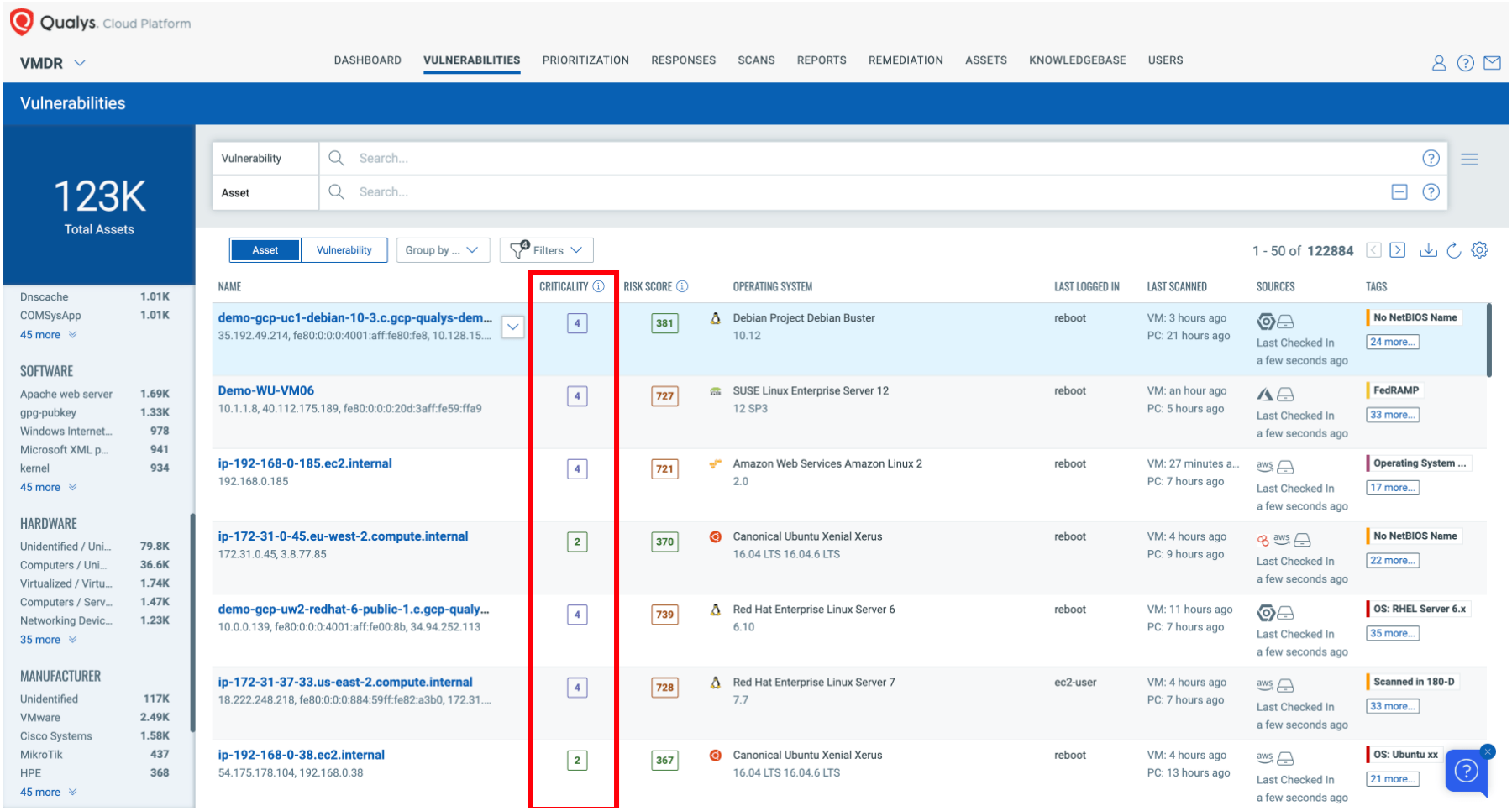
The previous examples were evaluating single vulnerabilities.



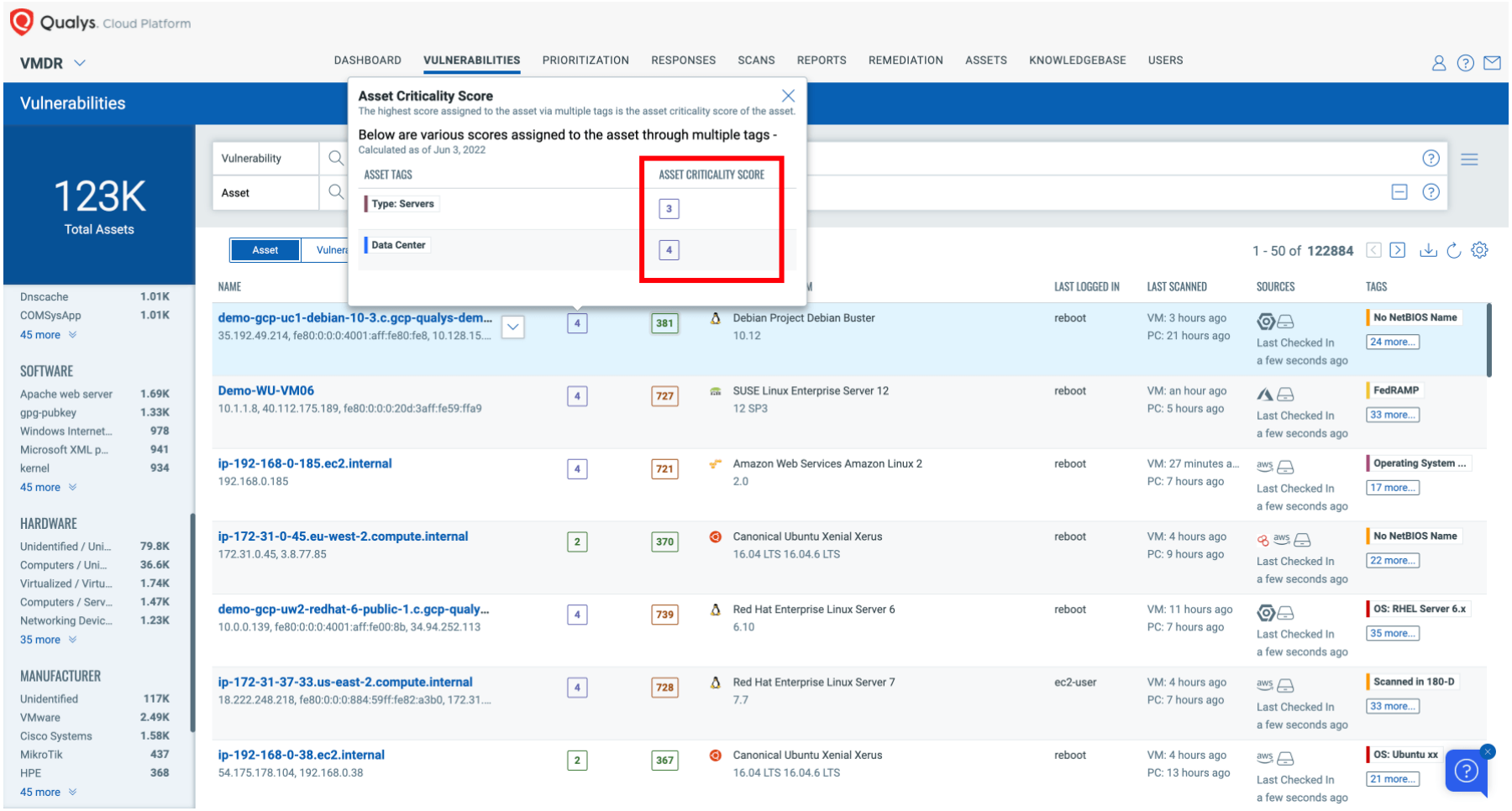
The steps that will follow will consider the overall health of the asset itself. Click Asset to change the dataset viewing.



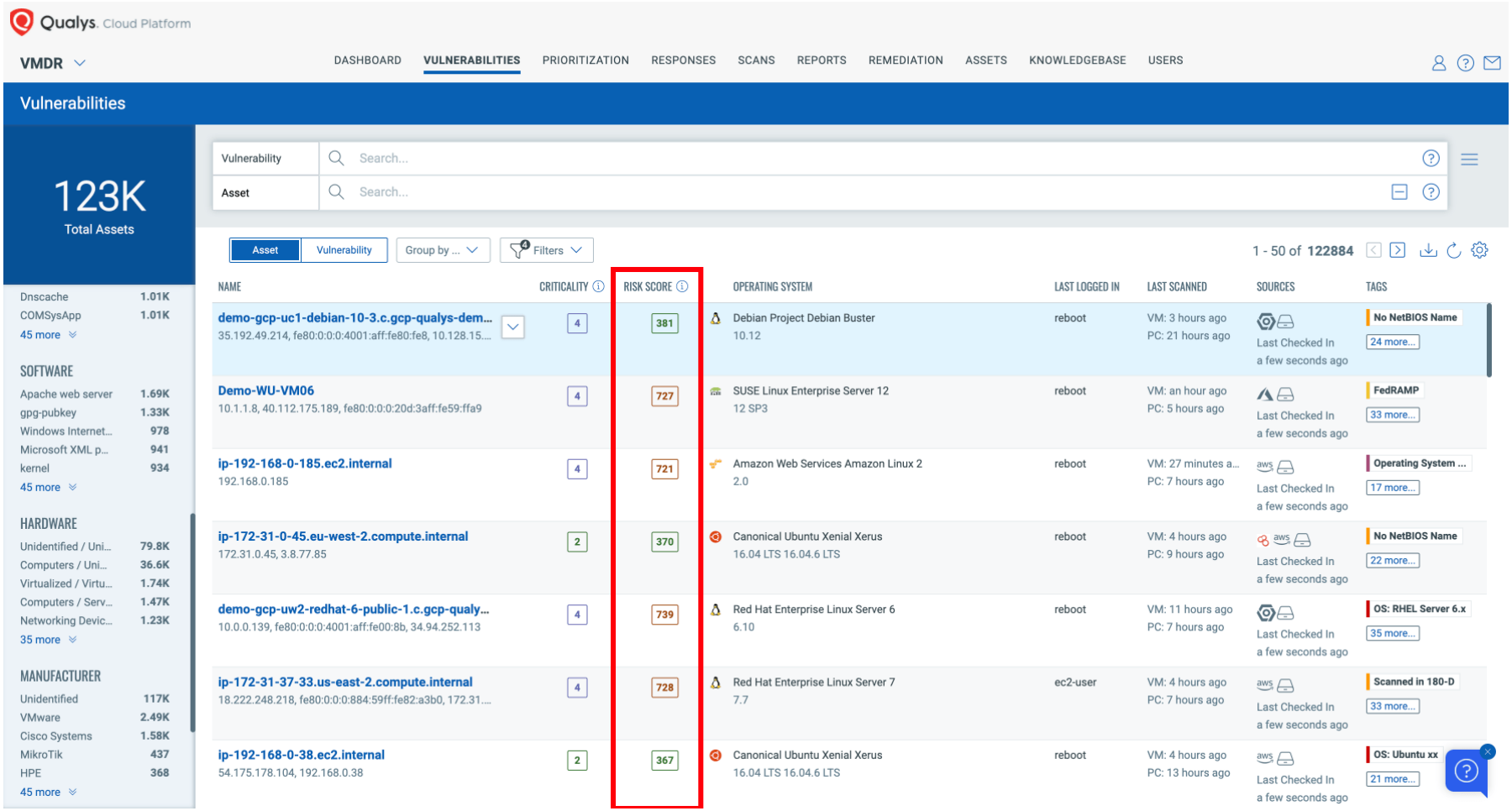
You influence the level of importance of your assets by setting the criticality of asset tags. The Asset Criticality value is the highest of all the tags assigned to the asset.



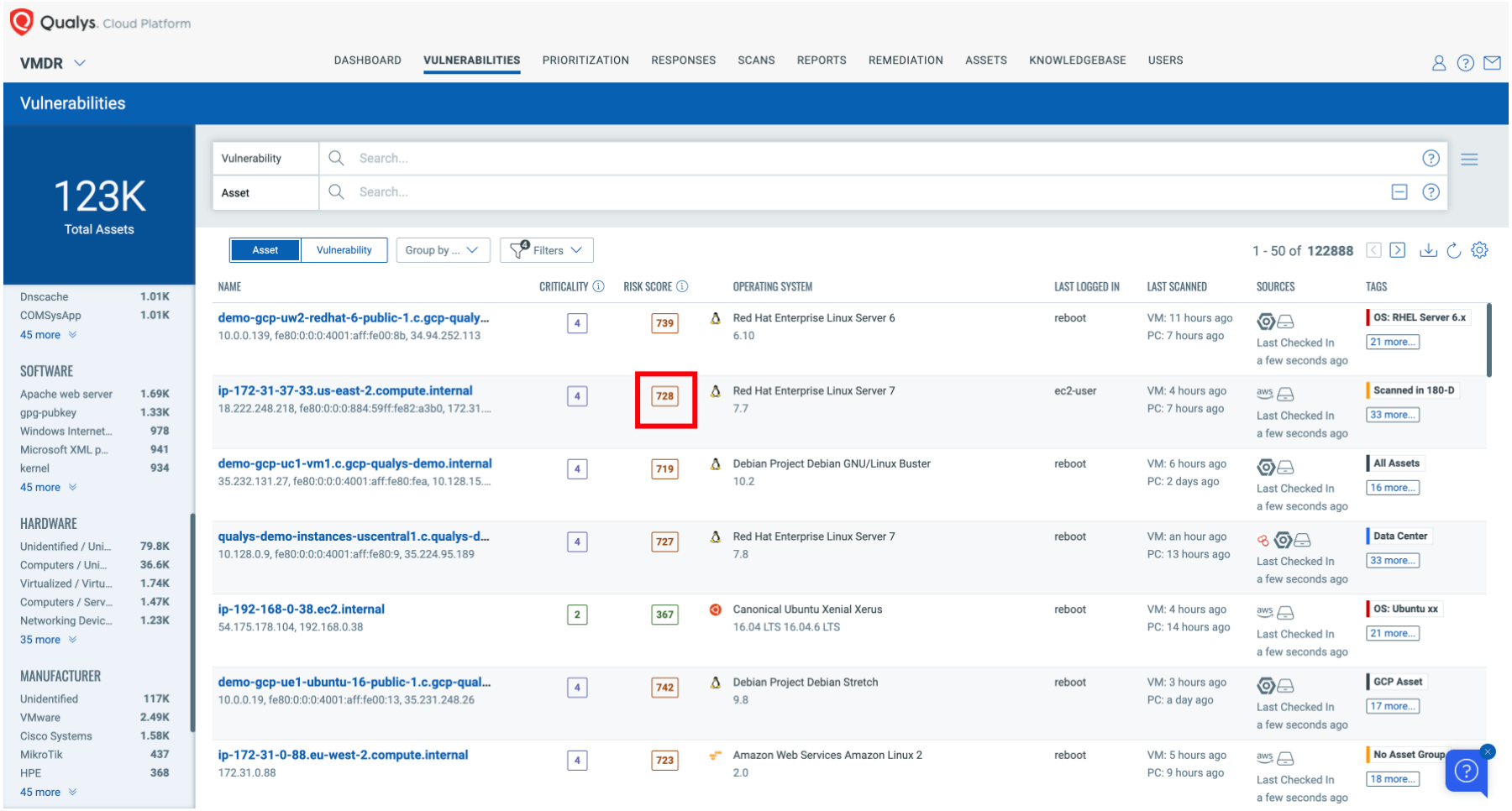
Here you will see that the Asset Criticality of 4 is due to the Data Center tag's criticality. This is because it is the highest of the assigned tags.



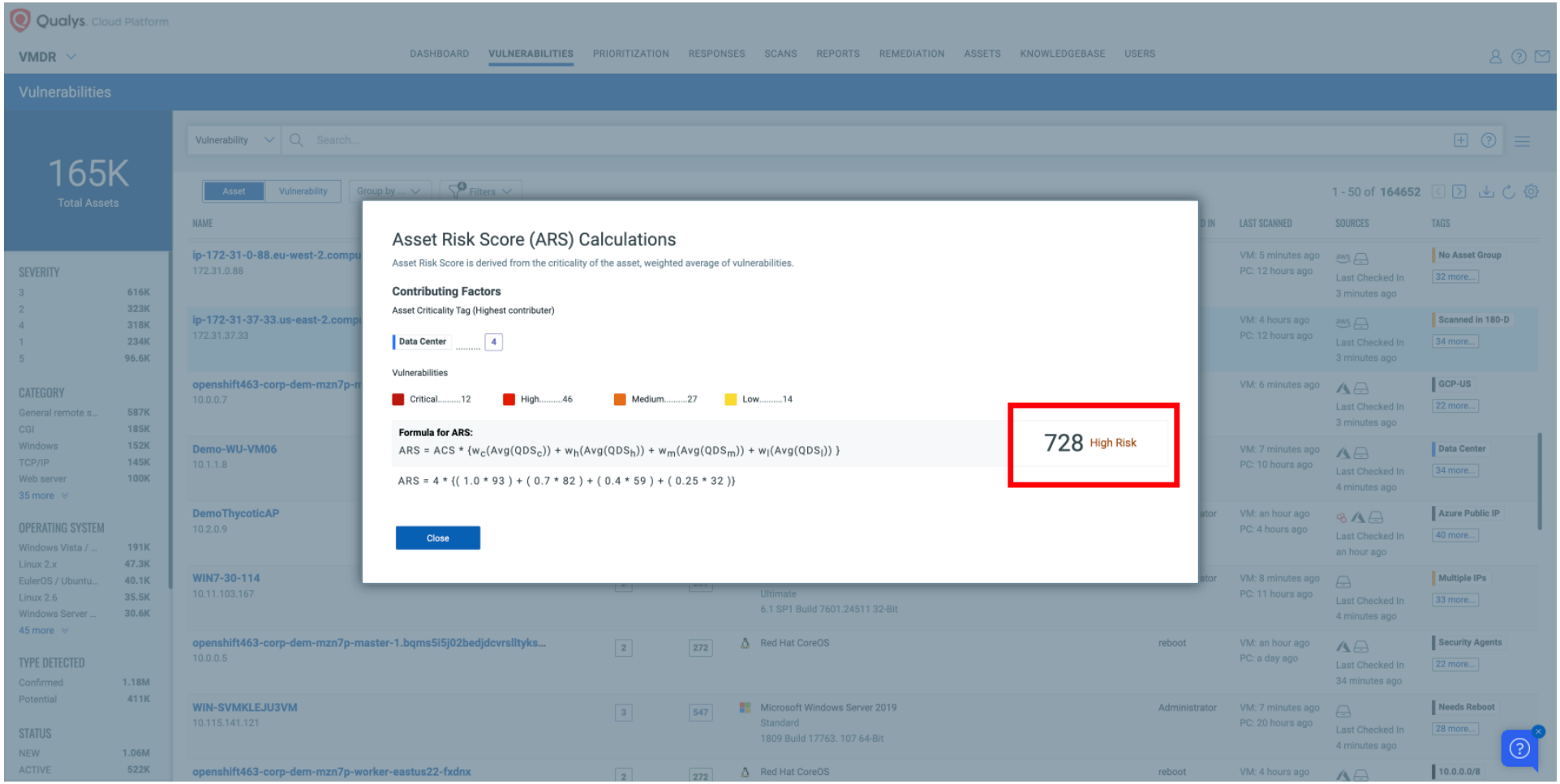
The Risk Score for the asset brings together the Asset Criticality and the QDS of all detected vulnerabilities on the asset. The overall health of the asset is reflected in this value.



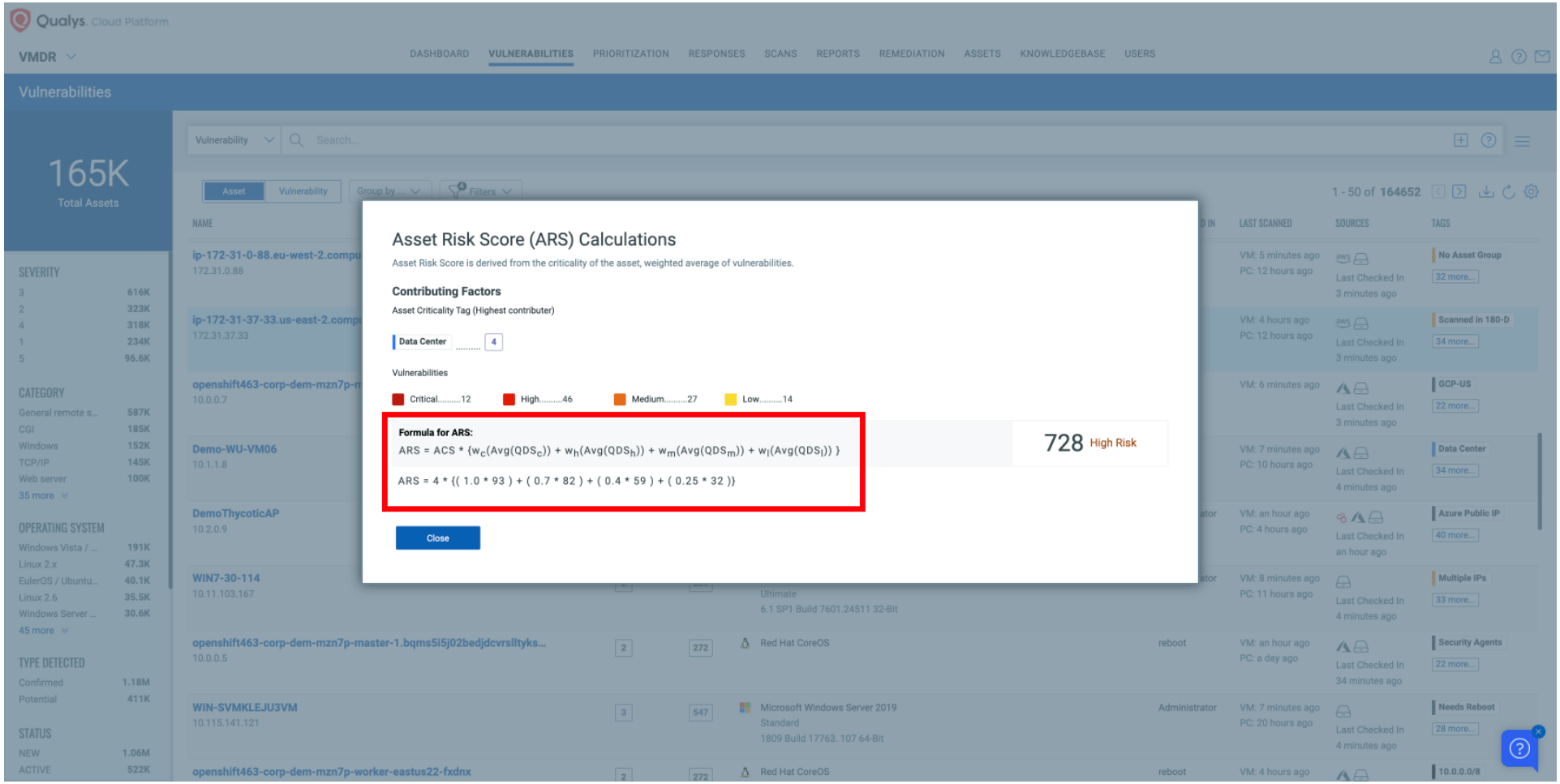
The steps to follow will show how the highlighted Risk Score is calculated.



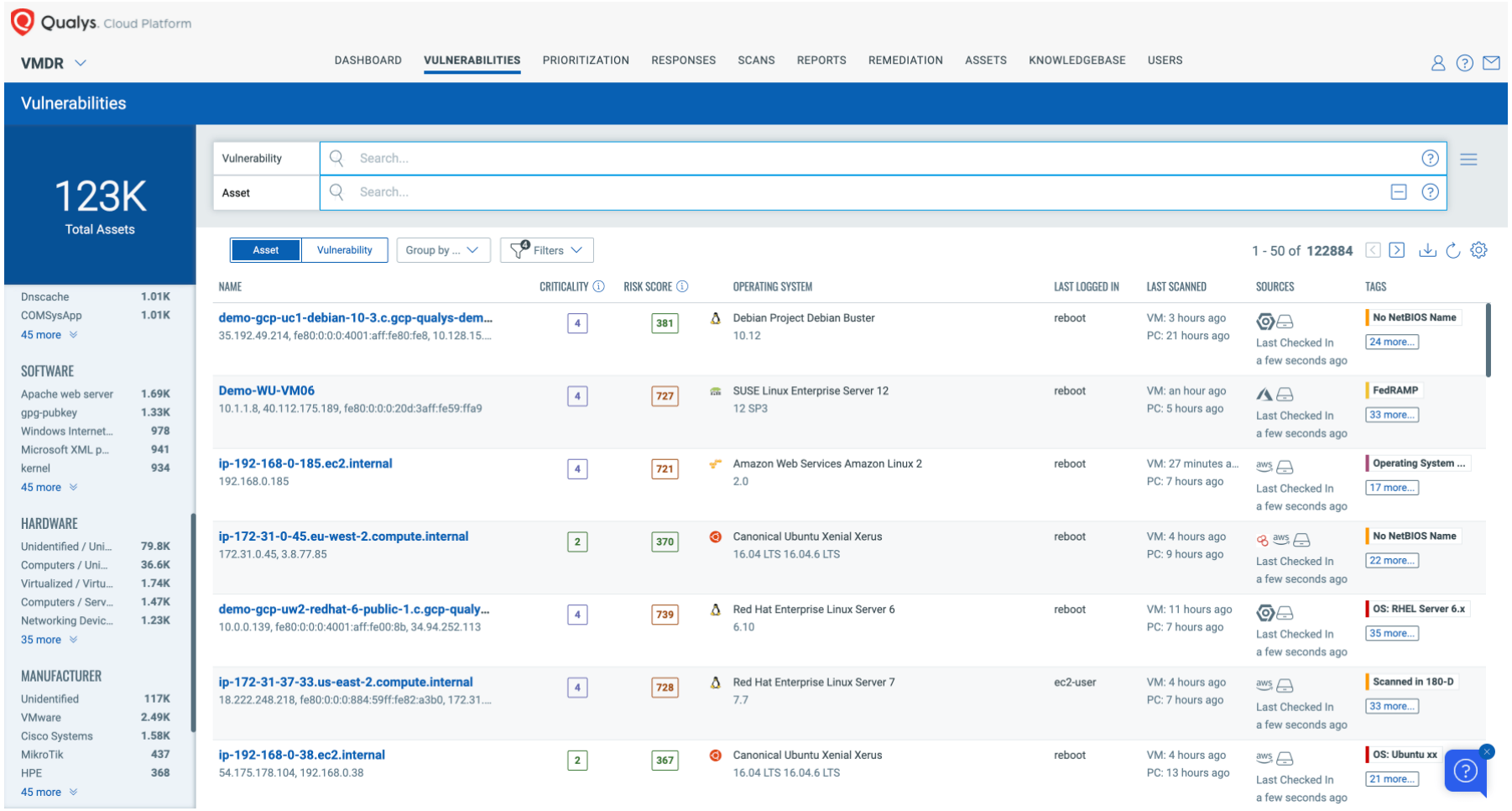
The Asset Risk Score can range from 0 to 1000 based on different factors. A score of 850 and above warrants immediate remediation measures to be taken on that asset.



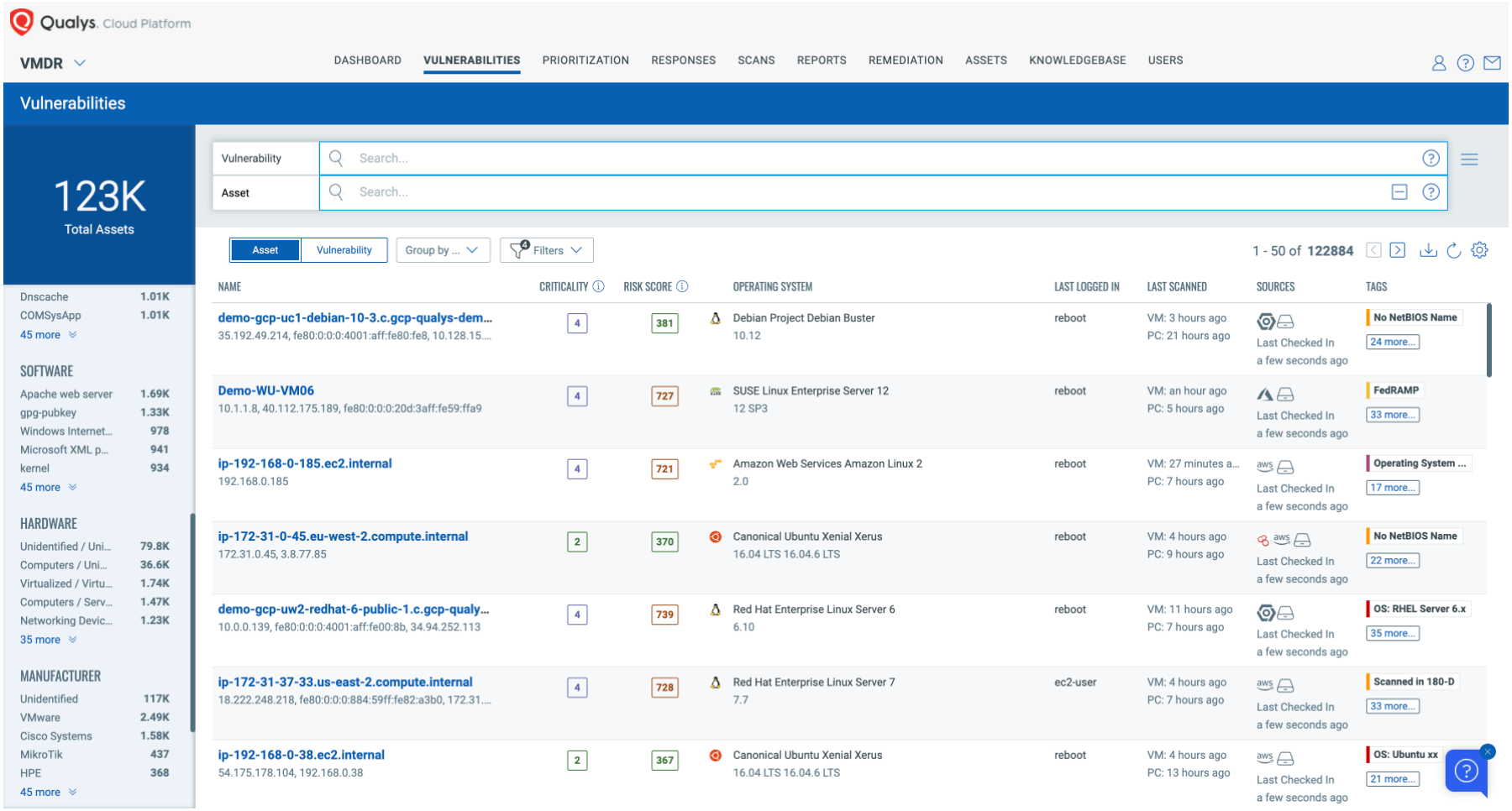
The Asset Criticality Score (ACS) is combined with a weighted average of its combined vulnerability detections. This is the formula and calculation you see.



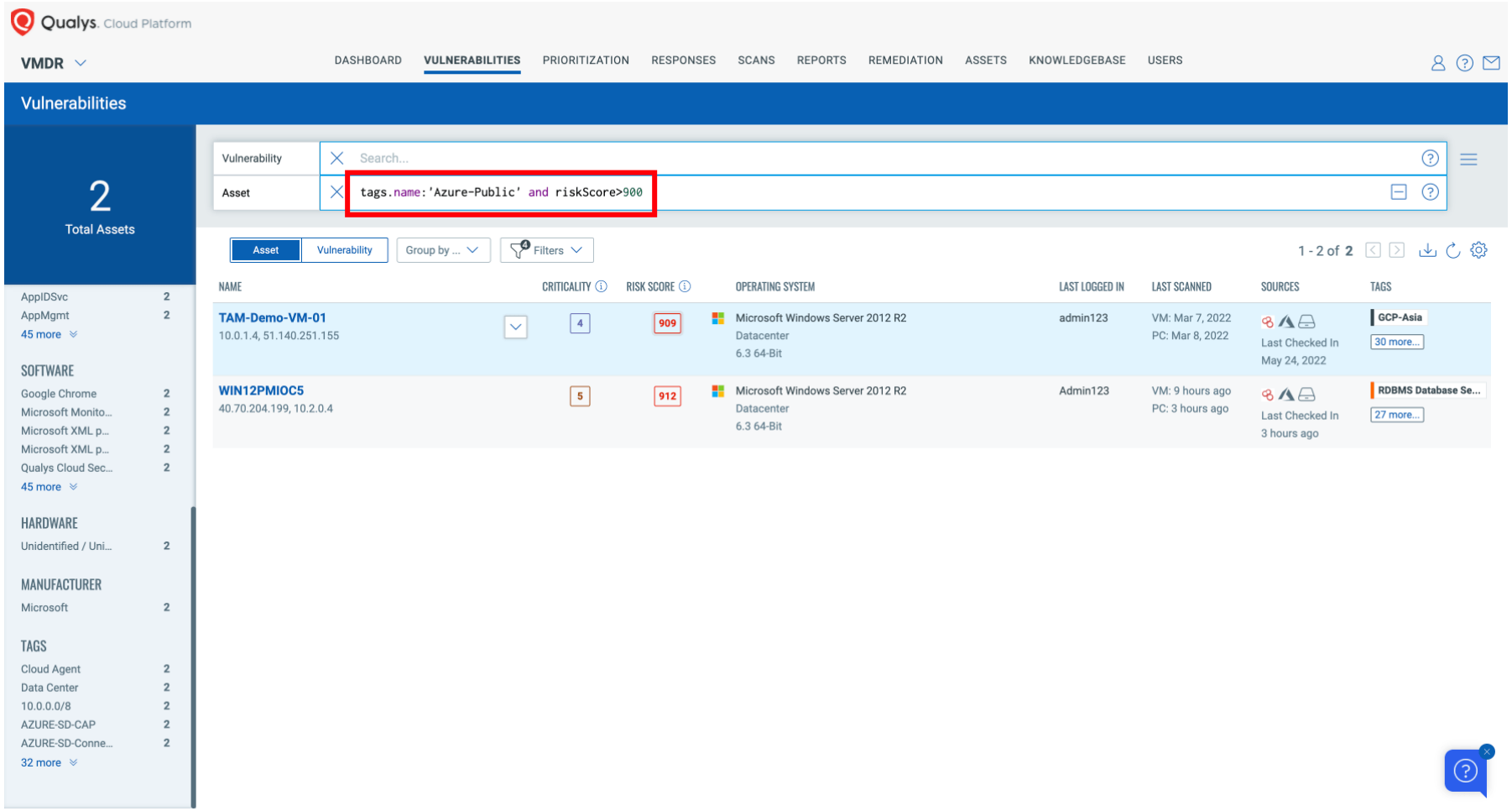
The steps to follow presents a use case to query a specific set of assets.



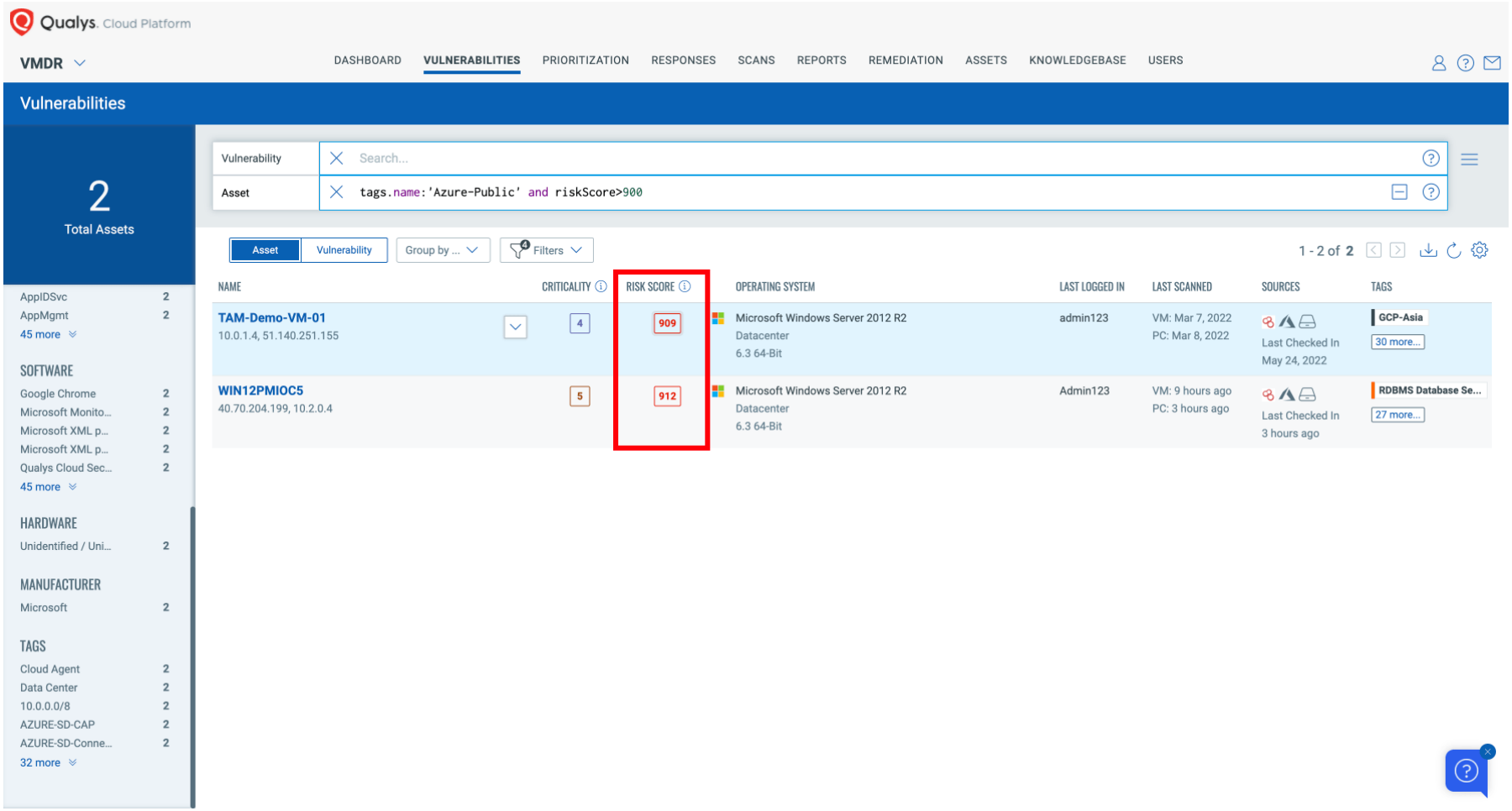
Let us say we want to find out our Azure public assets with a risk score of more than 900. This will reflect which of our public-facing cloud assets that need immediate action.



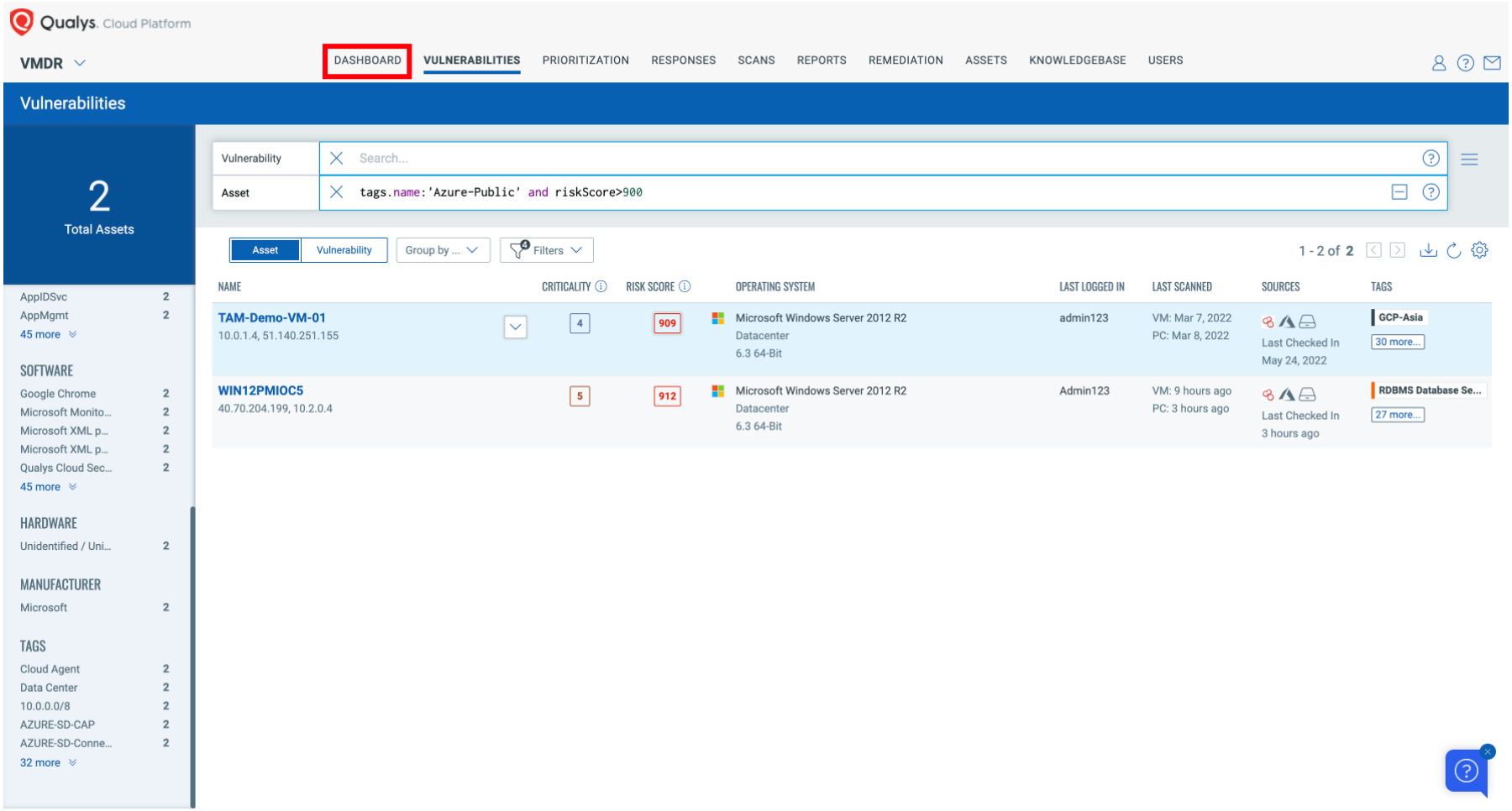
Here you see the query to produce our dataset.



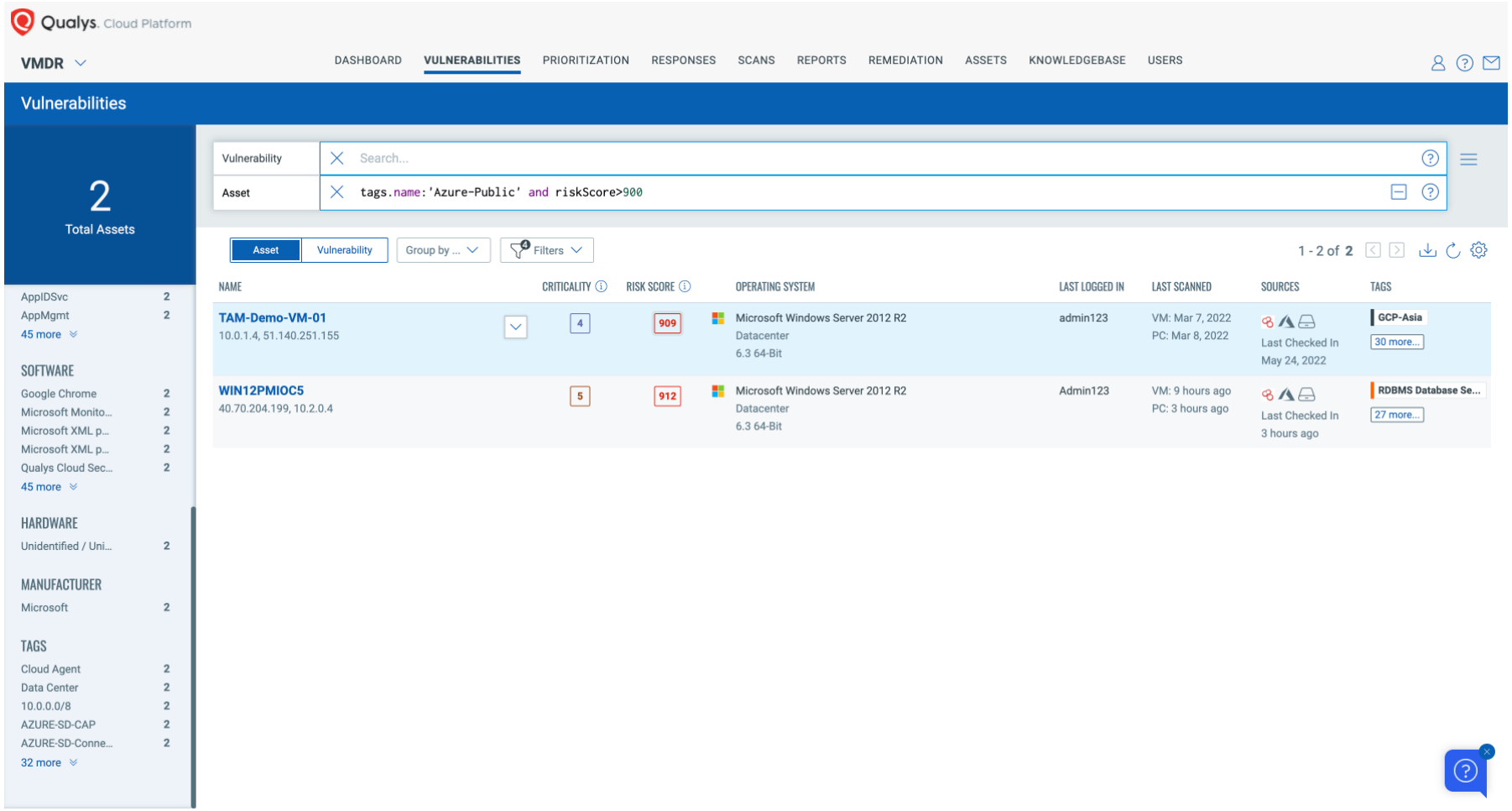
Two assets have Risk Scores requiring immediate attention. From this example, you can use queries like this to find assets that pose the highest risk to your organization.



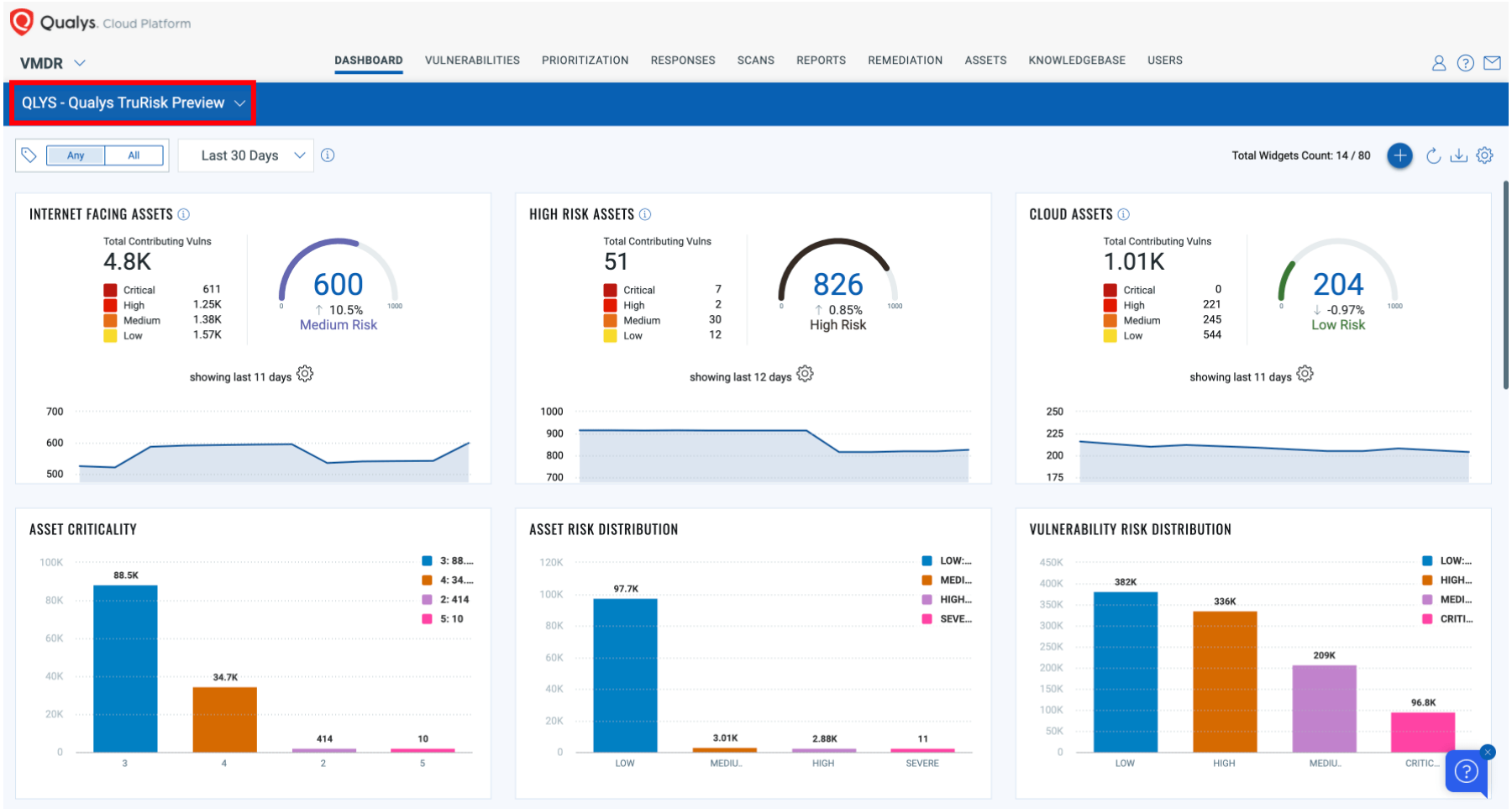
A better way of monitoring and visualizing this data would be through the use of dashboards and widgets.



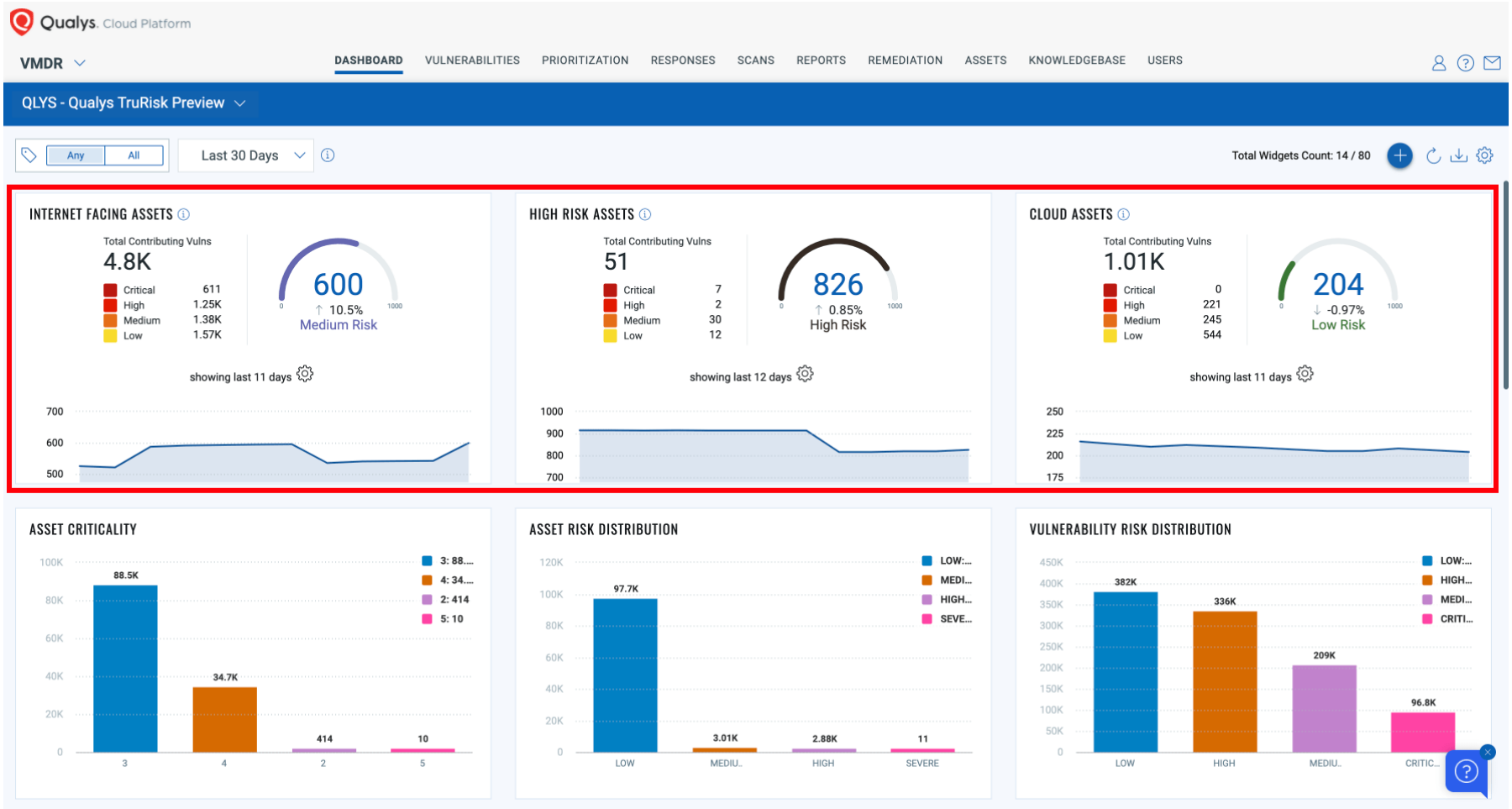
Click Dashboard.



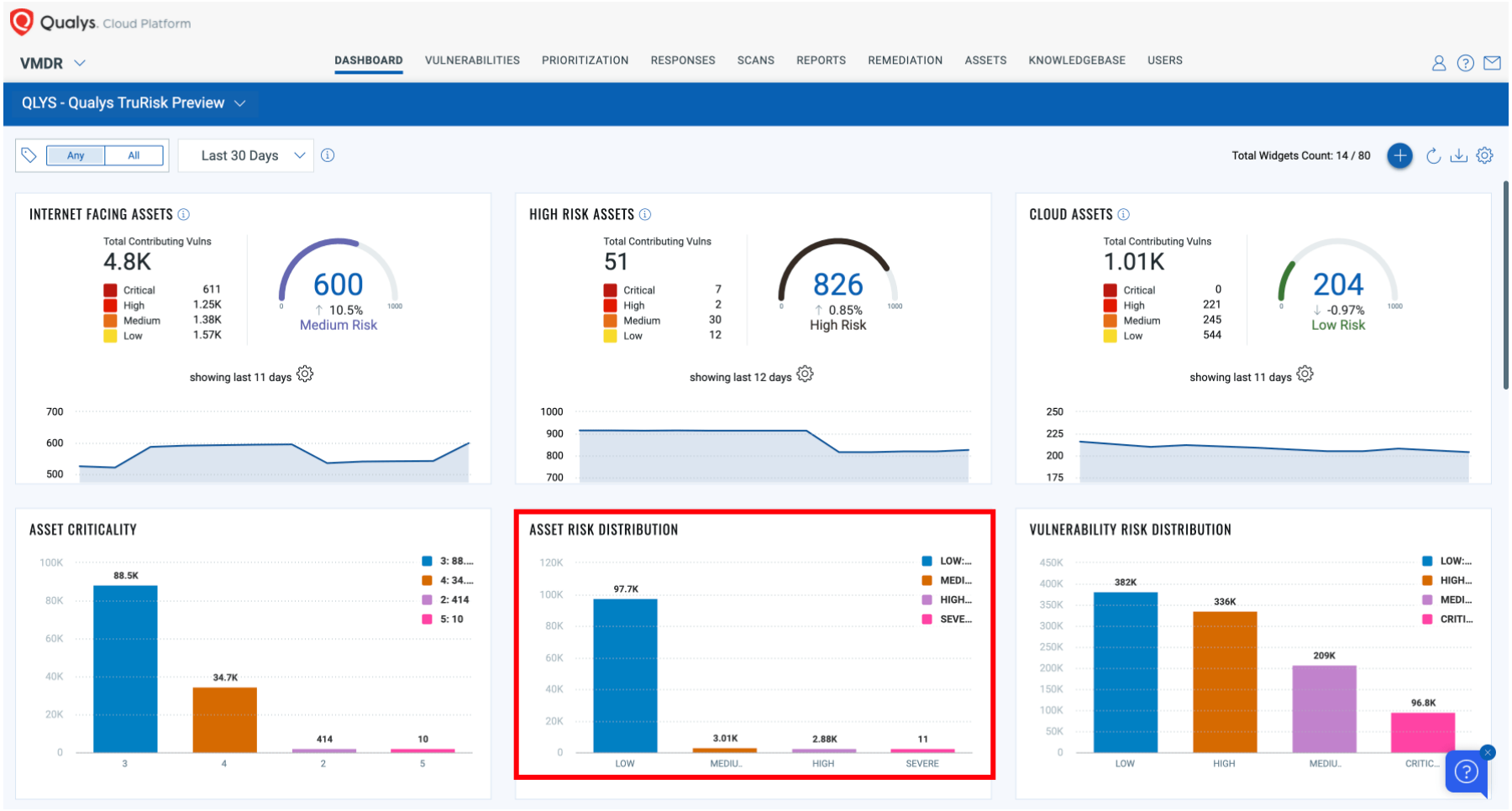
The Qualys TruRisk Dashboard has widgets where you can view a real-time picture of the assets that pose the greatest risk to your organization.



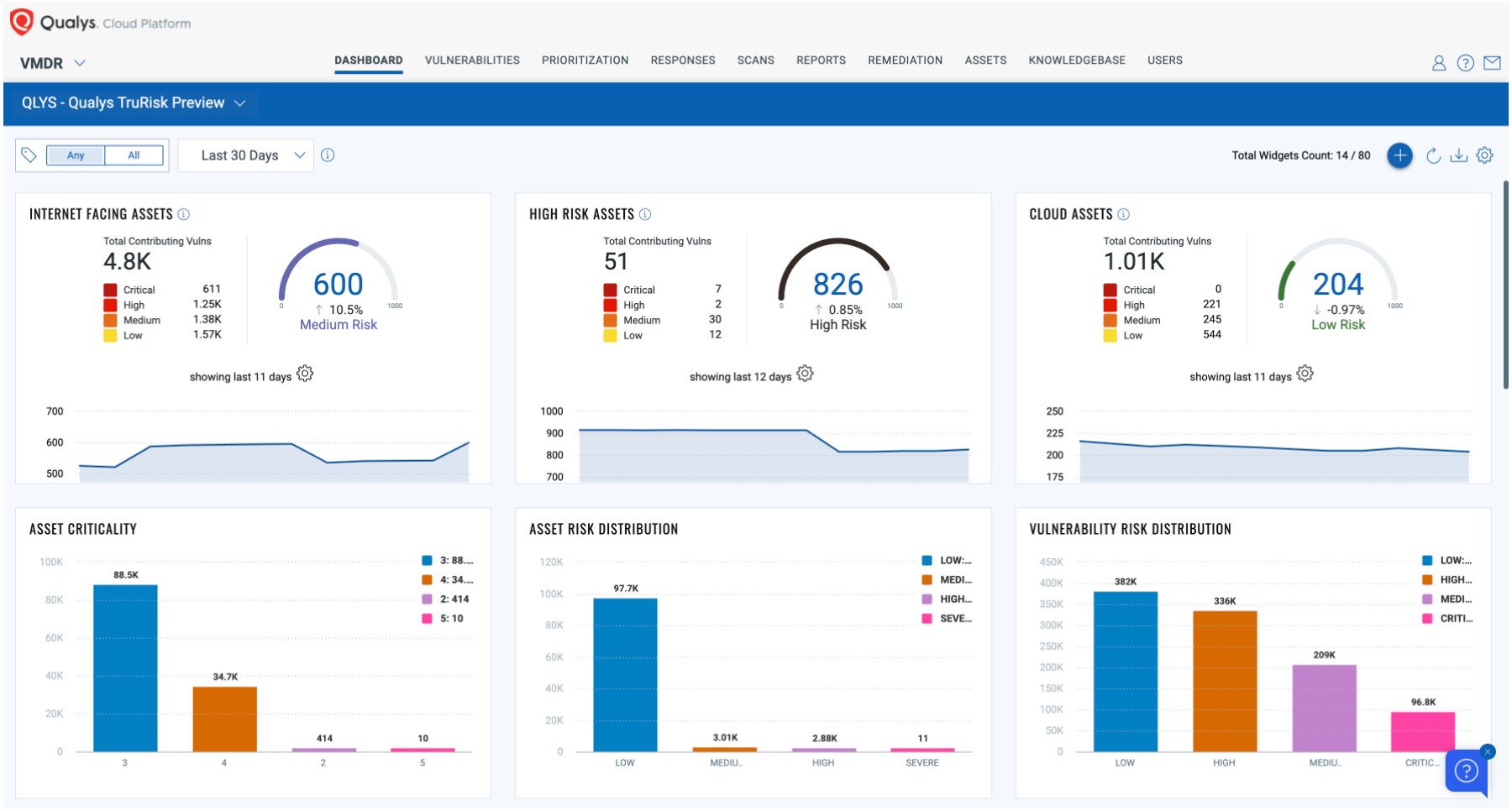
You can create many different widgets to visually monitor. Here you see widgets monitoring Risk Scores for Internet-facing assets, high risk assets, and cloud assets.



Additional out-of-box widgets are included that show a distribution of assets based on the TruRisk components. For example, the highlighted widget reflects the distribution of assets by their Risk Scores.


Qualys. Cloud Platform
VMDR
DASHBOARD
VULNERABILITIES
PRIORITIZATION
RESPONSES
SCANS
REPORTS
REMEDIATION
ASSETS
KNOWLEDGEBASE
USERS
QLYS - Qualys TruRisk Preview
Any
All
Last 30 Days
Total Widgets Count: 14 / 80
INTERNET FACING ASSETS
Total Contributing Vulns
4.8K
Critical 611
High 1.25K
Medium 1.38K
Low 1.57K
600
↑ 10.5%
Medium Risk
showing last 11 days
HIGH RISK ASSETS
Total Contributing Vulns
51
Critical 7
High 2
Medium 30
Low 12
826
↑ 0.85%
High Risk
showing last 12 days
CLOUD ASSETS
Total Contributing Vulns
1.01K
Critical 0
High 221
Medium 245
Low 544
204
↓ -0.97%
Low Risk
showing last 11 days
ASSET CRITICALITY
88.5K
34.7K
414
10
ASSET RISK DISTRIBUTION
97.7K
3.01K
2.88K
11
LOW
MEDIU..
HIGH
SEVERE
VULNERABILITY RISK DISTRIBUTION
382K
336K
209K
96.8K
LOW
HIGH
MEDIU..
CRITIC..

That's it. You're done.



Scan to go to the interactive player