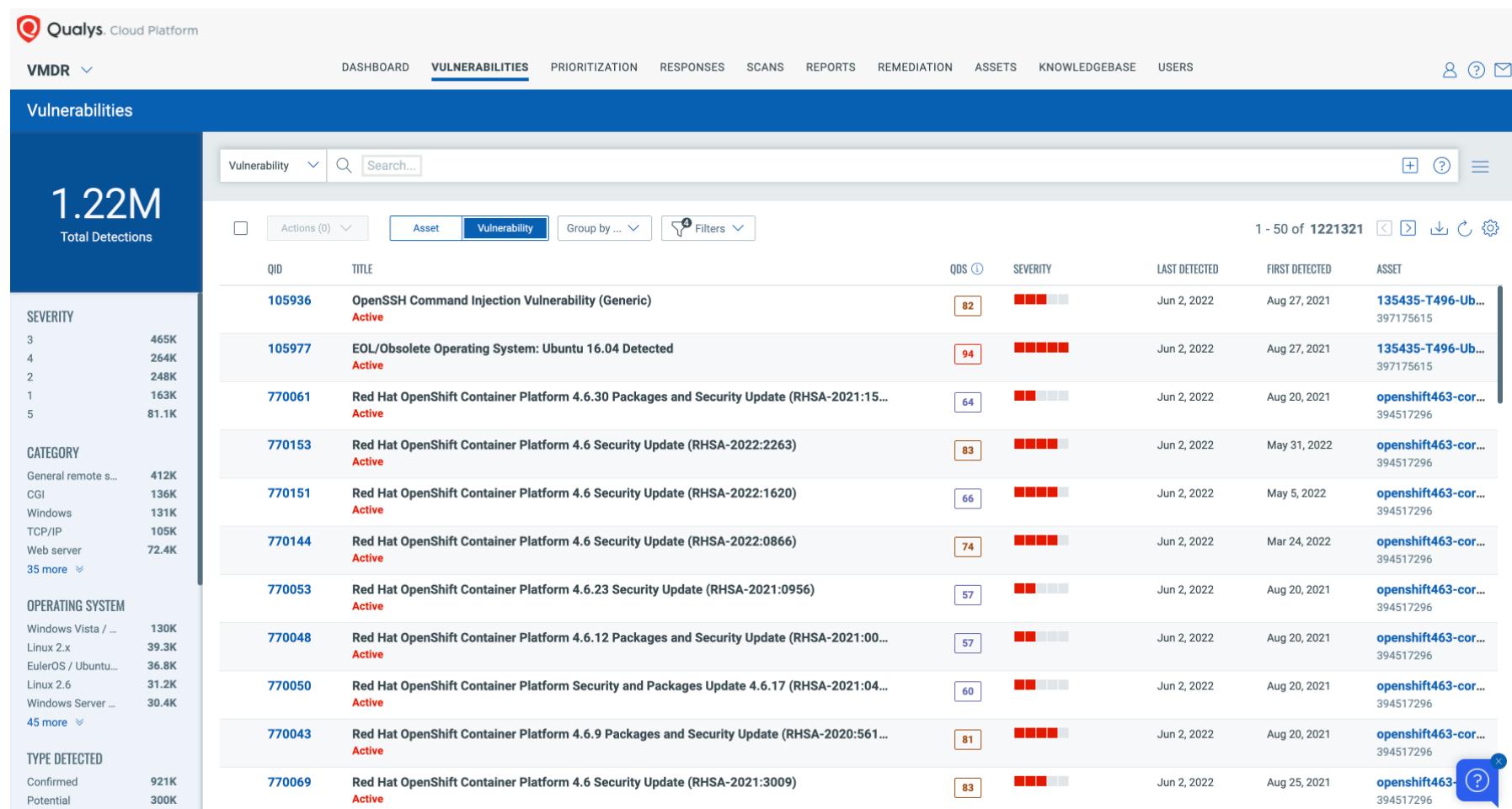


i Based on your environment, you can have many vulnerabilities ranging from a few hundred, to millions. It is important to understand the need to prioritize, and which should be remediated first.

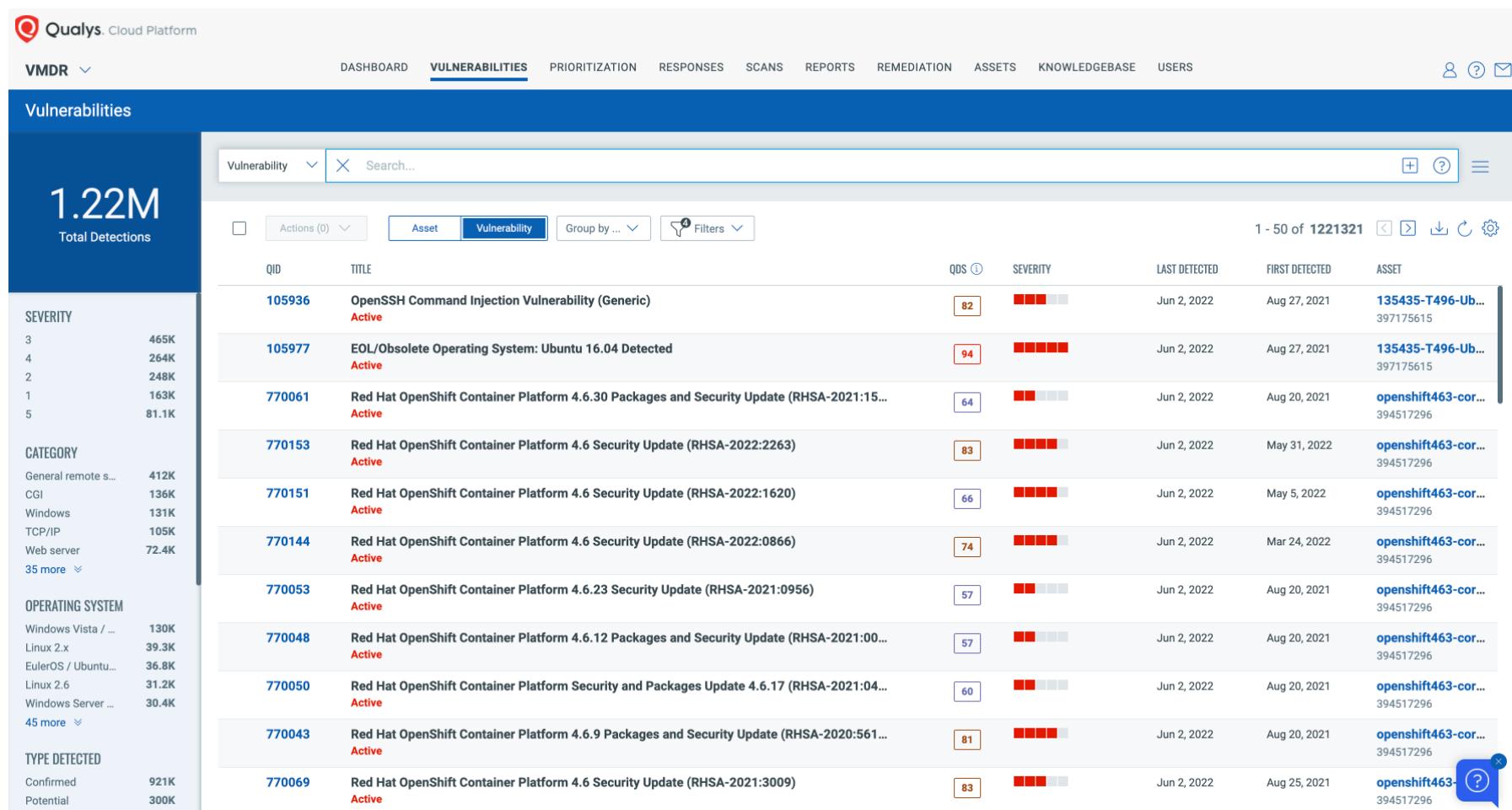


The screenshot shows the Qualys Cloud Platform VMDR interface. The main header includes the Qualys logo, navigation tabs (VMDR, DASHBOARD, VULNERABILITIES, PRIORITIZATION, RESPONSES, SCANS, REPORTS, REMEDIATION, ASSETS, KNOWLEDGEBASE, USERS), and user icons. The 'VULNERABILITIES' tab is selected.

A prominent blue sidebar on the left displays key statistics: **1.22M Total Detections**, followed by sections for **SEVERITY** (with counts for 3, 4, 2, 1, 5), **CATEGORY** (General remote s..., CGI, Windows, TCP/IP, Web server, 35 more), **OPERATING SYSTEM** (Windows Vista / ..., Linux 2.x, EulerOS / Ubuntu..., Linux 2.6, Windows Server ...), and **TYPE DETECTED** (Confirmed, Potential).

The main content area is titled 'Vulnerabilities' and shows a table of 1-50 of 1221321 results. The columns include QID, TITLE, QDS (with a value of 82 highlighted in orange), SEVERITY (with a severity bar), LAST DETECTED, FIRST DETECTED, and ASSET (with a link to '135435-T496-Ub...'). The table lists various Red Hat OpenShift Container Platform vulnerabilities, such as 'OpenSSH Command Injection Vulnerability (Generic)' and multiple security updates for Red Hat OpenShift Container Platform 4.6.

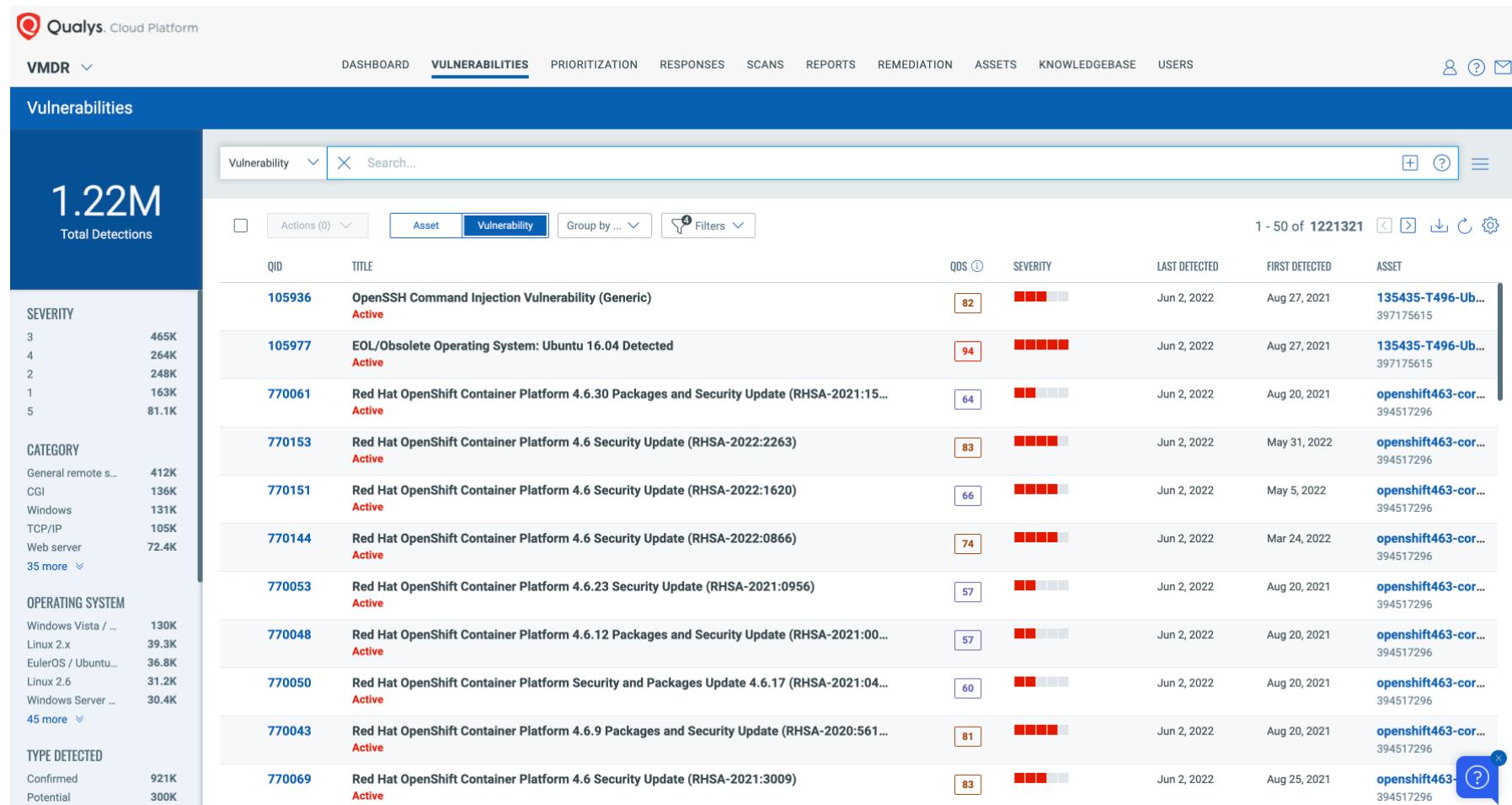
- 1 Historically, organizations have relied on CVSS scores. This is only effective to a certain point. A CVSS score does not include external factors like exploit kits or recent exploit trends.



The screenshot shows the Qualys Cloud Platform interface, specifically the 'Vulnerabilities' section. The top navigation bar includes links for DASHBOARD, VULNERABILITIES (which is underlined), PRIORITIZATION, RESPONSES, SCANS, REPORTS, REMEDIATION, ASSETS, KNOWLEDGEBASE, and USERS. On the left, there's a sidebar with filters for 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), and TYPE DETECTED (Confirmed 921K, Potential 300K). The main area displays a table of vulnerabilities with columns: QID, TITLE, QDS (with a value of 82 for the first item), SEVERITY (represented by a red bar chart), LAST DETECTED (Jun 2, 2022), FIRST DETECTED (Aug 27, 2021), and ASSET (135435-T496-Ub... 397175615). The first few rows list various Red Hat OpenShift Container Platform security updates, all marked as 'Active'. A search bar at the top right contains the placeholder 'Search...'.

QID	TITLE	QDS	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
105936	OpenSSH Command Injection Vulnerability (Generic Active)	82	<div style="width: 82%; background-color: red;"></div>	Jun 2, 2022	Aug 27, 2021	135435-T496-Ub... 397175615
105977	EOL/Obsolete Operating System: Ubuntu 16.04 Detected Active	94	<div style="width: 94%; background-color: red;"></div>	Jun 2, 2022	Aug 27, 2021	135435-T496-Ub... 397175615
770061	Red Hat OpenShift Container Platform 4.6.30 Packages and Security Update (RHSA-2021:15... Active	64	<div style="width: 64%; background-color: red;"></div>	Jun 2, 2022	Aug 20, 2021	openshift463-cor... 394517296
770153	Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2022:2263) Active	83	<div style="width: 83%; background-color: red;"></div>	Jun 2, 2022	May 31, 2022	openshift463-cor... 394517296
770151	Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2022:1620) Active	66	<div style="width: 66%; background-color: red;"></div>	Jun 2, 2022	May 5, 2022	openshift463-cor... 394517296
770144	Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2022:0866) Active	74	<div style="width: 74%; background-color: red;"></div>	Jun 2, 2022	Mar 24, 2022	openshift463-cor... 394517296
770053	Red Hat OpenShift Container Platform 4.6.23 Security Update (RHSA-2021:0956) Active	57	<div style="width: 57%; background-color: red;"></div>	Jun 2, 2022	Aug 20, 2021	openshift463-cor... 394517296
770048	Red Hat OpenShift Container Platform 4.6.12 Packages and Security Update (RHSA-2021:00... Active	57	<div style="width: 57%; background-color: red;"></div>	Jun 2, 2022	Aug 20, 2021	openshift463-cor... 394517296
770050	Red Hat OpenShift Container Platform Security and Packages Update 4.6.17 (RHSA-2021:04... Active	60	<div style="width: 60%; background-color: red;"></div>	Jun 2, 2022	Aug 20, 2021	openshift463-cor... 394517296
770043	Red Hat OpenShift Container Platform 4.6.9 Packages and Security Update (RHSA-2020:561... Active	81	<div style="width: 81%; background-color: red;"></div>	Jun 2, 2022	Aug 20, 2021	openshift463-cor... 394517296
770069	Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:3009) Active	83	<div style="width: 83%; background-color: red;"></div>	Jun 2, 2022	Aug 25, 2021	openshift463- 394517296

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



The screenshot shows the Qualys Cloud Platform interface, specifically the Vulnerabilities section. On the left, there's a sidebar with metrics: 1.22M Total Detections, a Severity breakdown (3: 465K, 4: 264K, 2: 248K, 1: 163K, 5: 81.1K), a Category breakdown (General remote s... 412K, CGI 136K, Windows 131K, TCP/IP 105K, Web server 72.4K, 35 more ...), an Operating System breakdown (Windows Vista / ... 130K, Linux 2.x 39.3K, EulerOS / Ubuntu... 36.8K, Linux 2.6 31.2K, Windows Server ... 30.4K, 45 more ...), and a Type Detected breakdown (Confirmed 921K, Potential 300K). The main area displays a table of vulnerabilities with columns: QID, TITLE, ODS (with a tooltip), SEVERITY (represented by a bar chart), LAST DETECTED, FIRST DETECTED, and ASSET. The first few rows show vulnerabilities related to OpenSSH, EOL/Obsolete Operating Systems, and Red Hat OpenShift Container Platform updates.

QID	TITLE	ODS	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
105936	OpenSSH Command Injection Vulnerability (Generic) Active	82	<div style="width: 82%;">███████</div>	Jun 2, 2022	Aug 27, 2021	135435-T496-Ub... 397175615
105977	EOL/Obsolete Operating System: Ubuntu 16.04 Detected Active	94	<div style="width: 94%;">██████████</div>	Jun 2, 2022	Aug 27, 2021	135435-T496-Ub... 397175615
770061	Red Hat OpenShift Container Platform 4.6.30 Packages and Security Update (RHSA-2021:15... Active	64	<div style="width: 64%;">███████</div>	Jun 2, 2022	Aug 20, 2021	openshift463-cor... 394517296
770153	Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2022:2263) Active	83	<div style="width: 83%;">███████</div>	Jun 2, 2022	May 31, 2022	openshift463-cor... 394517296
770151	Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2022:1620) Active	66	<div style="width: 66%;">███████</div>	Jun 2, 2022	May 5, 2022	openshift463-cor... 394517296
770144	Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2022:0866) Active	74	<div style="width: 74%;">███████</div>	Jun 2, 2022	Mar 24, 2022	openshift463-cor... 394517296
770053	Red Hat OpenShift Container Platform 4.6.23 Security Update (RHSA-2021:0956) Active	57	<div style="width: 57%;">███████</div>	Jun 2, 2022	Aug 20, 2021	openshift463-cor... 394517296
770048	Red Hat OpenShift Container Platform 4.6.12 Packages and Security Update (RHSA-2021:00... Active	57	<div style="width: 57%;">███████</div>	Jun 2, 2022	Aug 20, 2021	openshift463-cor... 394517296
770050	Red Hat OpenShift Container Platform Security and Packages Update 4.6.17 (RHSA-2021:04... Active	60	<div style="width: 60%;">███████</div>	Jun 2, 2022	Aug 20, 2021	openshift463-cor... 394517296
770043	Red Hat OpenShift Container Platform 4.6.9 Packages and Security Update (RHSA-2020:561... Active	81	<div style="width: 81%;">███████</div>	Jun 2, 2022	Aug 20, 2021	openshift463-cor... 394517296
770069	Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:3009) Active	83	<div style="width: 83%;">███████</div>	Jun 2, 2022	Aug 25, 2021	openshift463- 394517296

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

The screenshot shows the Qualys Cloud Platform interface, specifically the Vulnerabilities section. A search bar at the top contains the query: `vulnerabilities.vulnerability.cvss2Info.baseScore<7`. This query filters the results to show only vulnerabilities with a base score of 7 or less. The results table displays various Microsoft security advisories, such as ADV190023, ADV190013, and ADV180012, along with their details like severity, last detected date, and first detected date. The interface includes navigation buttons for page 1-50 of 939594, and a sidebar on the left provides summary statistics for Severity, Category, Operating System, and Type Detected.

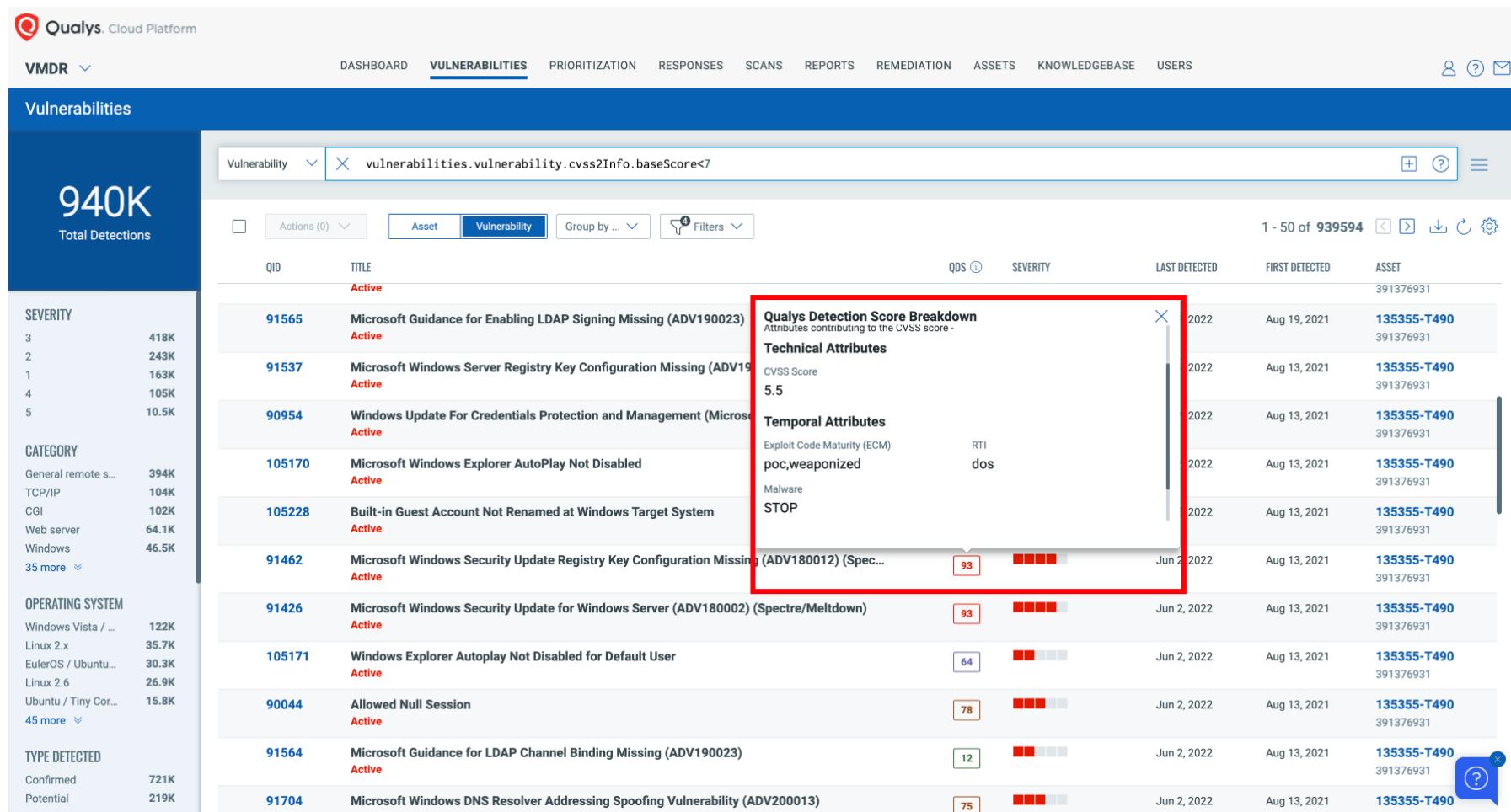
QID	Title	QDS	Severity	Last Detected	First Detected	Asset
91565	Microsoft Guidance for Enabling LDAP Signing Missing (ADV190023) Active	16	Medium	Jun 2, 2022	Aug 19, 2021	135355-T490 391376931
91537	Microsoft Windows Server Registry Key Configuration Missing (ADV190013) Active	31	Medium	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
90954	Windows Update For Credentials Protection and Management (Microsoft Security Advisory 2... Active	7	Medium	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
105170	Microsoft Windows Explorer AutoPlay Not Disabled Active	64	Medium	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
105228	Built-in Guest Account Not Renamed at Windows Target System Active	6	Medium	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91462	Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spec... Active	93	Medium	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91426	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown) Active	93	Medium	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
105171	Windows Explorer Autoplay Not Disabled for Default User Active	64	Medium	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
90044	Allowed Null Session Active	78	Medium	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91564	Microsoft Guidance for LDAP Channel Binding Missing (ADV190023) Active	12	Medium	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91704	Microsoft Windows DNS Resolver Addressing Spoofing Vulnerability (ADV200013)	75	Medium	Jun 2, 2022	Aug 13, 2021	135355-T490

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

The screenshot shows the Qualys Cloud Platform interface, specifically the 'Vulnerabilities' section. The main header includes the Qualys logo, navigation tabs (VMDR, DASHBOARD, VULNERABILITIES, PRIORITIZATION, RESPONSES, SCANS, REPORTS, REMEDIATION, ASSETS, KNOWLEDGEBASE, USERS), and user icons. A search bar at the top contains the query: 'vulnerabilities.vulnerability.cvss2Info.baseScore<7'. The left sidebar displays summary statistics: 940K Total Detections, a Severity breakdown (3: 418K, 2: 243K, 1: 163K, 4: 105K, 5: 10.5K), a Category breakdown (General remote s...: 394K, TCP/IP: 104K, CGI: 102K, Web server: 64.1K, Windows: 46.5K, 35 more...), an Operating System breakdown (Windows Vista / ...: 122K, Linux 2.x: 35.7K, EulerOS / Ubuntu...: 30.3K, Linux 2.6: 26.9K, Ubuntu / Tiny Cor...: 15.8K, 45 more...), and a Type Detected breakdown (Confirmed: 721K, Potential: 219K). The main content area shows a table of vulnerabilities with columns: QID, TITLE, QDS, SEVERITY, LAST DETECTED, FIRST DETECTED, and ASSET. The first row, which is highlighted with a red box, is for vulnerability 91462: 'Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spec... Active'. It has a QID of 91462, a title of 'Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spec...', a QDS of 93, a severity of 4 (red), and was last detected on Jun 2, 2022, first detected on Aug 13, 2021, and is associated with asset 391376931. Other visible rows include 91565, 91537, 90954, 105170, 105228, 91426, 105171, 90044, 91564, and 91704.

QID	TITLE	QDS	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
91462	Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spec... Active	93	4	Jun 2, 2022	Aug 13, 2021	391376931
91565	Microsoft Guidance for Enabling LDAP Signing Missing (ADV190023) Active	16	3	Jun 2, 2022	Aug 19, 2021	391376931
91537	Microsoft Windows Server Registry Key Configuration Missing (ADV190013) Active	31	3	Jun 2, 2022	Aug 13, 2021	391376931
90954	Windows Update For Credentials Protection and Management (Microsoft Security Advisory 2... Active	7	3	Jun 2, 2022	Aug 13, 2021	391376931
105170	Microsoft Windows Explorer AutoPlay Not Disabled Active	64	3	Jun 2, 2022	Aug 13, 2021	391376931
105228	Built-in Guest Account Not Renamed at Windows Target System Active	6	3	Jun 2, 2022	Aug 13, 2021	391376931
91426	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown) Active	93	3	Jun 2, 2022	Aug 13, 2021	391376931
105171	Windows Explorer Autoplay Not Disabled for Default User Active	64	3	Jun 2, 2022	Aug 13, 2021	391376931
90044	Allowed Null Session Active	78	3	Jun 2, 2022	Aug 13, 2021	391376931
91564	Microsoft Guidance for LDAP Channel Binding Missing (ADV190023) Active	12	3	Jun 2, 2022	Aug 13, 2021	391376931
91704	Microsoft Windows DNS Resolver Addressing Spoofing Vulnerability (ADV200013) Active	75	3	Jun 2, 2022	Aug 13, 2021	391376931

- 1 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.



The screenshot shows the Qualys Cloud Platform interface under the 'VULNERABILITIES' tab. A search bar at the top contains the query: 'vulnerabilities.vulnerability.cvss2Info.baseScore<7'. The main table lists various vulnerabilities with columns for QID, TITLE, QDS (Qualys Detection Score), SEVERITY, LAST DETECTED, FIRST DETECTED, and ASSET. One specific row for 'Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012)' is highlighted with a red box. This row shows a QDS score of 93, which is also highlighted with a red box. The 'Qualys Detection Score Breakdown' section for this vulnerability includes 'Technical Attributes' (CVSS Score: 5.5) and 'Temporal Attributes' (Exploit Code Maturity (ECM): poc, Malware: STOP). The 'ASSET' column for this row shows the ID 391376931.

QID	TITLE	QDS	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
91565	Microsoft Guidance for Enabling LDAP Signing Missing (ADV190023)	93	Low	Jun 2, 2022	Aug 19, 2021	135355-T490 391376931
91537	Microsoft Windows Server Registry Key Configuration Missing (ADV190023)	93	Low	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
90954	Windows Update For Credentials Protection and Management (Micros... Active	93	Low	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
105170	Microsoft Windows Explorer AutoPlay Not Disabled	93	Low	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
105228	Built-in Guest Account Not Renamed at Windows Target System Active	93	Low	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91462	Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spec... Active	93	Low	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91426	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown) Active	93	Low	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
105171	Windows Explorer Autoplay Not Disabled for Default User Active	64	Low	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
90044	Allowed Null Session Active	78	Low	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91564	Microsoft Guidance for LDAP Channel Binding Missing (ADV190023) Active	12	Low	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91704	Microsoft Windows DNS Resolver Addressing Spoofing Vulnerability (ADV200013)	75	Low	Jun 2, 2022	Aug 13, 2021	135355-T490

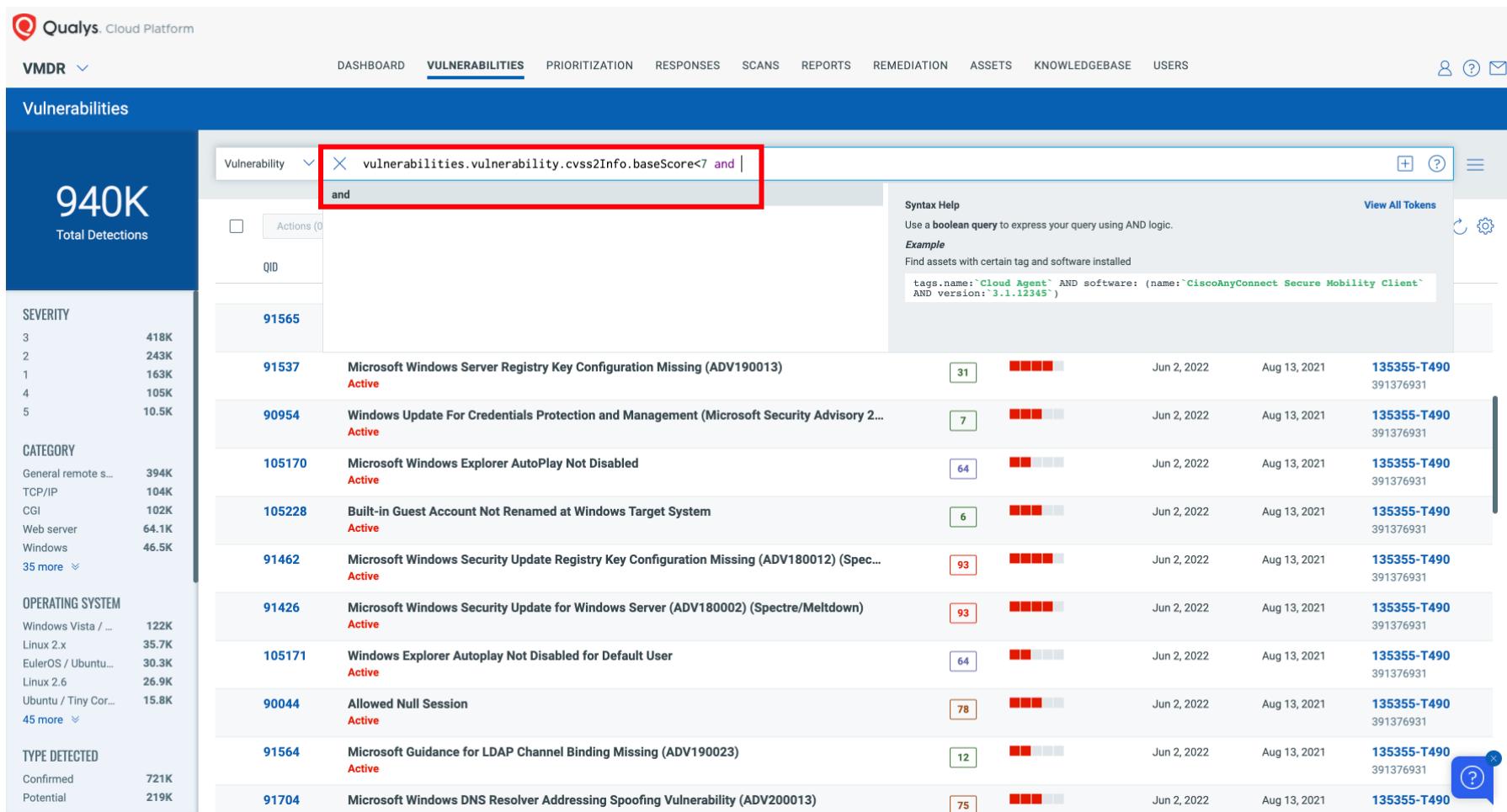
1 This is why Qualys has developed the Qualys Detection Score. QDS takes CVSS as a key input and adds temporal factors to reflect the risk level of a vulnerability to your organization.

The screenshot shows the Qualys Cloud Platform interface with the 'VULNERABILITIES' tab selected. The main dashboard displays a total of 940K detections. On the left, there are filters for Severity (3, 2, 1, 4, 5) and Category (General remote s..., TCP/IP, CGI, Web server, Windows), along with operating system and type detected details. The central part of the screen shows a table of vulnerabilities with columns for QID, Title, QDS (highlighted by a red box), Severity, Last Detected, First Detected, and Asset. The QDS column contains numerical values ranging from 16 to 93, indicating the detection score for each vulnerability.

QID	TITLE	QDS	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
91565	Microsoft Guidance for Enabling LDAP Signing Missing (ADV190023) Active	16	Medium	Jun 2, 2022	Aug 19, 2021	135355-T490 391376931
91537	Microsoft Windows Server Registry Key Configuration Missing (ADV190013) Active	31	High	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
90954	Windows Update For Credentials Protection and Management (Microsoft Security Advisory 2... Active	7	Medium	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
105170	Microsoft Windows Explorer AutoPlay Not Disabled Active	64	High	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
105228	Built-in Guest Account Not Renamed at Windows Target System Active	6	Medium	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91462	Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spec... Active	93	High	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91426	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown) Active	93	High	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
105171	Windows Explorer Autoplay Not Disabled for Default User Active	64	Medium	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
90044	Allowed Null Session Active	78	High	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91564	Microsoft Guidance for LDAP Channel Binding Missing (ADV190023) Active	12	Medium	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91704	Microsoft Windows DNS Resolver Addressing Spoofing Vulnerability (ADV200013)	75	High	Jun 2, 2022	Aug 13, 2021	135355-T490

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

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



The screenshot shows the Qualys Cloud Platform interface, specifically the Vulnerabilities section. A search bar at the top contains the query: `vulnerabilities.vulnerability.cvss2Info.baseScore<7 and`. A red box highlights this part of the query. To the right of the search bar is a syntax help panel with the following text:

```

Syntax Help
Use a boolean query to express your query using AND logic.

Example
Find assets with certain tag and software installed
tags.name:Cloud Agent AND software: (name: CiscoAnyConnect Secure Mobility Client AND version: 3.1.12345)

```

The main table below the search bar lists various vulnerabilities with their details such as ID, title, severity, and remediation status. The first few rows are:

ID	Title	Severity	Remediation Status	Last Update	Created	Tags
91537	Microsoft Windows Server Registry Key Configuration Missing (ADV190013) Active	3	31	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
90954	Windows Update For Credentials Protection and Management (Microsoft Security Advisory 2... Active	2	7	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
105170	Microsoft Windows Explorer AutoPlay Not Disabled Active	1	64	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
105228	Built-in Guest Account Not Renamed at Windows Target System Active	4	6	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91462	Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spec... Active	5	93	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91426	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown) Active	3	93	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
105171	Windows Explorer Autoplay Not Disabled for Default User Active	4	64	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
90044	Allowed Null Session Active	5	78	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91564	Microsoft Guidance for LDAP Channel Binding Missing (ADV190023) Active	7	12	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91704	Microsoft Windows DNS Resolver Addressing Spoofing Vulnerability (ADV200013)	8	75	Jun 2, 2022	Aug 13, 2021	135355-T490

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

The screenshot shows the Qualys Cloud Platform interface with the 'VULNERABILITIES' tab selected. On the left, there's a summary card for '940K Total Detections' and filters for 'SEVERITY' (3, 2, 1, 4, 5), 'CATEGORY' (General remote s..., TCP/IP, CGI, Web server, Windows), 'OPERATING SYSTEM' (Windows Vista / ..., Linux 2.x, EulerOS / Ubuntu..., Linux 2.6, Ubuntu / Tiny Cor...), and 'TYPE DETECTED' (Confirmed, Potential). The main area displays a list of vulnerabilities with columns for ID, Title, Status, Score, Last Seen, First Seen, and Token. An example token 'vulnerabilities.detectionScore:[0..30]' is highlighted with a red box in the search bar's dropdown. A tooltip for this token explains it selects the number of days from the range (0..30, 31..60, 61..90, 91..180, 180..+) since the vulnerability was first detected by a scanner or cloud agent on the asset till the current date. The age is calculated irrespective of the vulnerability status. The token is also shown in the 'Example' section below the search bar.

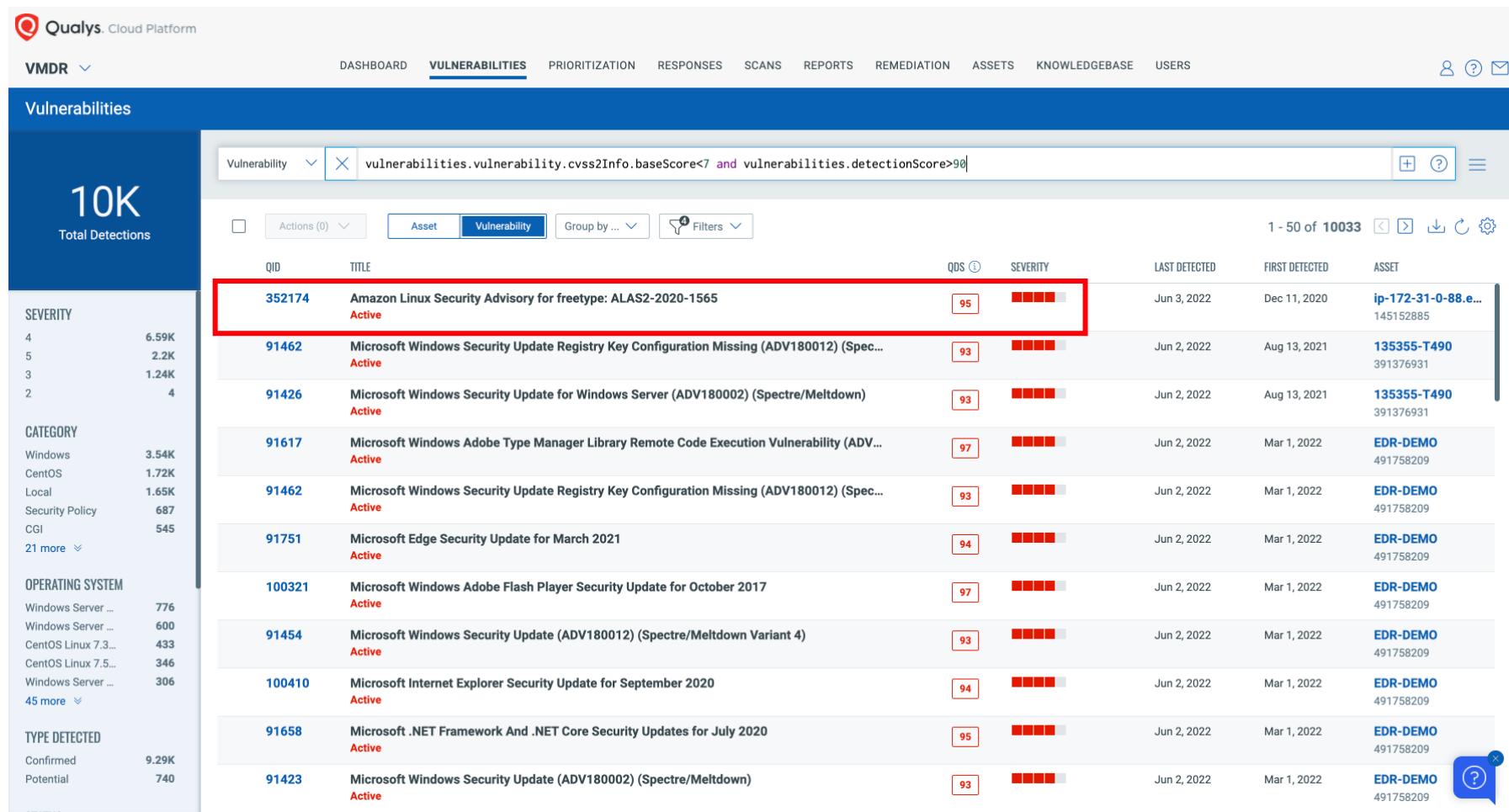
Vulnerability	vulnerabilities.detectionAge	vulnerabilities.detectionScore	vulnerabilities.typeDetected	Syntax Help	View All Tokens
91565	vulnerabilities.detectionAge	vulnerabilities.detectionScore	vulnerabilities.typeDetected	Select the number of days from the range (0..30, 31..60, 61..90, 91..180, 180..+) since the vulnerability was first detected (by a scanner or cloud agent) on the asset till the current date. The age is calculated irrespective of the vulnerability status.	View All Tokens
91537	Microsoft Windows Server Registry Key Configuration Missing (ADV190013) Active	31	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
90954	Windows Update For Credentials Protection and Management (Microsoft Security Advisory 2... Active	7	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
105170	Microsoft Windows Explorer AutoPlay Not Disabled Active	64	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
105228	Built-in Guest Account Not Renamed at Windows Target System Active	6	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
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
105171	Windows Explorer Autoplay Not Disabled for Default User Active	64	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
90044	Allowed Null Session Active	78	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91564	Microsoft Guidance for LDAP Channel Binding Missing (ADV190023) Active	12	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91704	Microsoft Windows DNS Resolver Addressing Spoofing Vulnerability (ADV200013) Active	75	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931

1 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.

The screenshot shows the Qualys Cloud Platform interface, specifically the VMDR section under the Vulnerabilities tab. A search bar at the top contains the query: `vulnerabilities.vulnerability.cvss2Info.baseScore<7 and vulnerabilities.detectionScore>90`. This query filters for vulnerabilities with a base CVSS score less than 7 and a detection score greater than 90. The results table displays 10033 findings, with the first 50 listed below. The columns include QID, Title, QDS (Qualys Detection Score), Severity, Last Detected, First Detected, and Asset. The results show various Microsoft Windows security updates and Adobe vulnerabilities, all marked as Active. The sidebar on the left provides summary statistics for 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, 600, CentOS Linux 7.3: 433, CentOS Linux 7.5: 346, Windows Server: 306, 45 more), and Type Detected (Confirmed: 9.29K, Potential: 740).

QID	TITLE	QDS	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
352174	Amazon Linux Security Advisory for freetype: ALAS2-2020-1565 Active	95	Medium	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	Medium	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91426	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown) Active	93	Medium	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91617	Microsoft Windows Adobe Type Manager Library Remote Code Execution Vulnerability (ADV... Active	97	Medium	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91462	Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spec... Active	93	Medium	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91751	Microsoft Edge Security Update for March 2021 Active	94	Medium	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
100321	Microsoft Windows Adobe Flash Player Security Update for October 2017 Active	97	Medium	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91454	Microsoft Windows Security Update (ADV180012) (Spectre/Meltdown Variant 4) Active	93	Medium	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
100410	Microsoft Internet Explorer Security Update for September 2020 Active	94	Medium	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91658	Microsoft .NET Framework And .NET Core Security Updates for July 2020 Active	95	Medium	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91423	Microsoft Windows Security Update (ADV180002) (Spectre/Meltdown) Active	93	Medium	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209

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



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)

QID	TITLE	QDS	Severity	Last Detected	First Detected	Asset
352174	Amazon Linux Security Advisory for freetype: ALAS2-2020-1565 Active	95	<div style="width: 95%;">██████</div>	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	<div style="width: 93%;">██████</div>	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91426	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown) Active	93	<div style="width: 93%;">██████</div>	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91617	Microsoft Windows Adobe Type Manager Library Remote Code Execution Vulnerability (ADV... Active	97	<div style="width: 97%;">███████</div>	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91462	Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spec... Active	93	<div style="width: 93%;">██████</div>	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91751	Microsoft Edge Security Update for March 2021 Active	94	<div style="width: 94%;">██████</div>	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
100321	Microsoft Windows Adobe Flash Player Security Update for October 2017 Active	97	<div style="width: 97%;">███████</div>	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91454	Microsoft Windows Security Update (ADV180012) (Spectre/Meltdown Variant 4) Active	93	<div style="width: 93%;">██████</div>	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
100410	Microsoft Internet Explorer Security Update for September 2020 Active	94	<div style="width: 94%;">██████</div>	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91658	Microsoft .NET Framework And .NET Core Security Updates for July 2020 Active	95	<div style="width: 95%;">██████</div>	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91423	Microsoft Windows Security Update (ADV180002) (Spectre/Meltdown) Active	93	<div style="width: 93%;">██████</div>	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209

- 1 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 VULNERABILITIES DASHBOARD PRIORITIZATION RESPONSES SEARCH

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  Actions (0) Asset Vulnerability Group by ... Filters

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)

1 - 50 of 10033

QID	TITLE	DETECTED	FIRST DETECTED	ASSET
352174	Amazon Linux Security Advisory for freetype: ALAS2-2020-1565 Active	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	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91426	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown) Active	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91617	Microsoft Windows Adobe Type Manager Library Remote Code Execution Vulnerability (ADV... Active	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91462	Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spec... Active	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91751	Microsoft Edge Security Update for March 2021 Active	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
100321	Microsoft Windows Adobe Flash Player Security Update for October 2017 Active	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91454	Microsoft Windows Security Update (ADV180012) (Spectre/Meltdown Variant 4) Active	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
100410	Microsoft Internet Explorer Security Update for September 2020 Active	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91658	Microsoft .NET Framework And .NET Core Security Updates for July 2020 Active	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91423	Microsoft Windows Security Update (ADV180002) (Spectre/Meltdown) Active	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209

- 1 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 VULNERABILITIES DASHBOARD PRIORITIZATION RESPONSES SEARCH

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  Exploit Code Maturity (ECM) poc,weaponized

Qualys Detection Score Breakdown  
CVSS Score 6.5

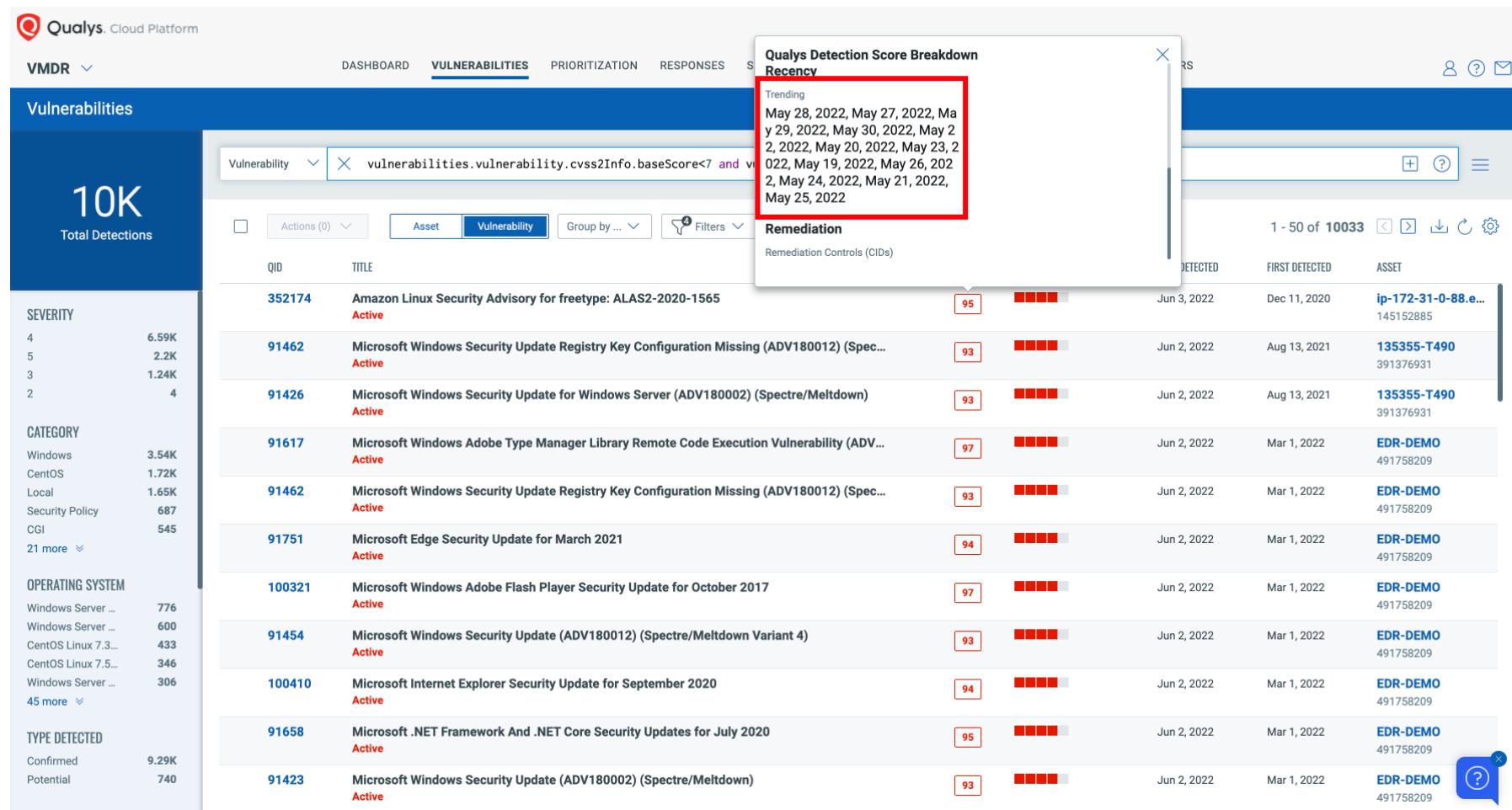
Temporal Attributes  
Exploit Code Maturity (ECM) poc,weaponized

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	Jun 3, 2022	Dec 11, 2020	ip-172-31-0-88.e... 145152885
352174	Amazon Linux Security Advisory for freetype: ALAS2-2020-1565 Active	Jun 2, 2022	Dec 11, 2020	ip-10-0-0-183.ec... 144957961
352174	Amazon Linux Security Advisory for freetype: ALAS2-2020-1565 Active	Jun 2, 2022	Dec 11, 2020	ip-192-168-0-185... 145132584
351339	Amazon Linux Security Advisory for kernel: ALAS-2018-1058 (FragmentSmack) Active	Apr 18, 2022	Sep 4, 2020	10.11.70.120 247763911
351178	Amazon Linux Security Advisory for kernel: ALAS-2018-956 Active	Apr 18, 2022	Sep 4, 2020	10.11.70.120 247763911
351270	Amazon Linux Security Advisory for kernel: ALAS-2018-1038 Active	Apr 18, 2022	Sep 4, 2020	10.11.70.120 247763911
351742	Amazon Linux Security Advisory for openssh: ALAS-2019-1313 Active	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	Apr 18, 2022	Sep 9, 2020	10.11.70.134 248867100
351178	Amazon Linux Security Advisory for kernel: ALAS-2018-956 Active	Apr 18, 2022	Sep 4, 2020	10.11.70.134 248867100
351270	Amazon Linux Security Advisory for kernel: ALAS-2018-1038 Active	Apr 18, 2022	Sep 4, 2020	10.11.70.134 248867100
351339	Amazon Linux Security Advisory for kernel: ALAS-2018-1058 (FragmentSmack) Active	Apr 18, 2022	Sep 4, 2020	10.11.70.134 248867100

1

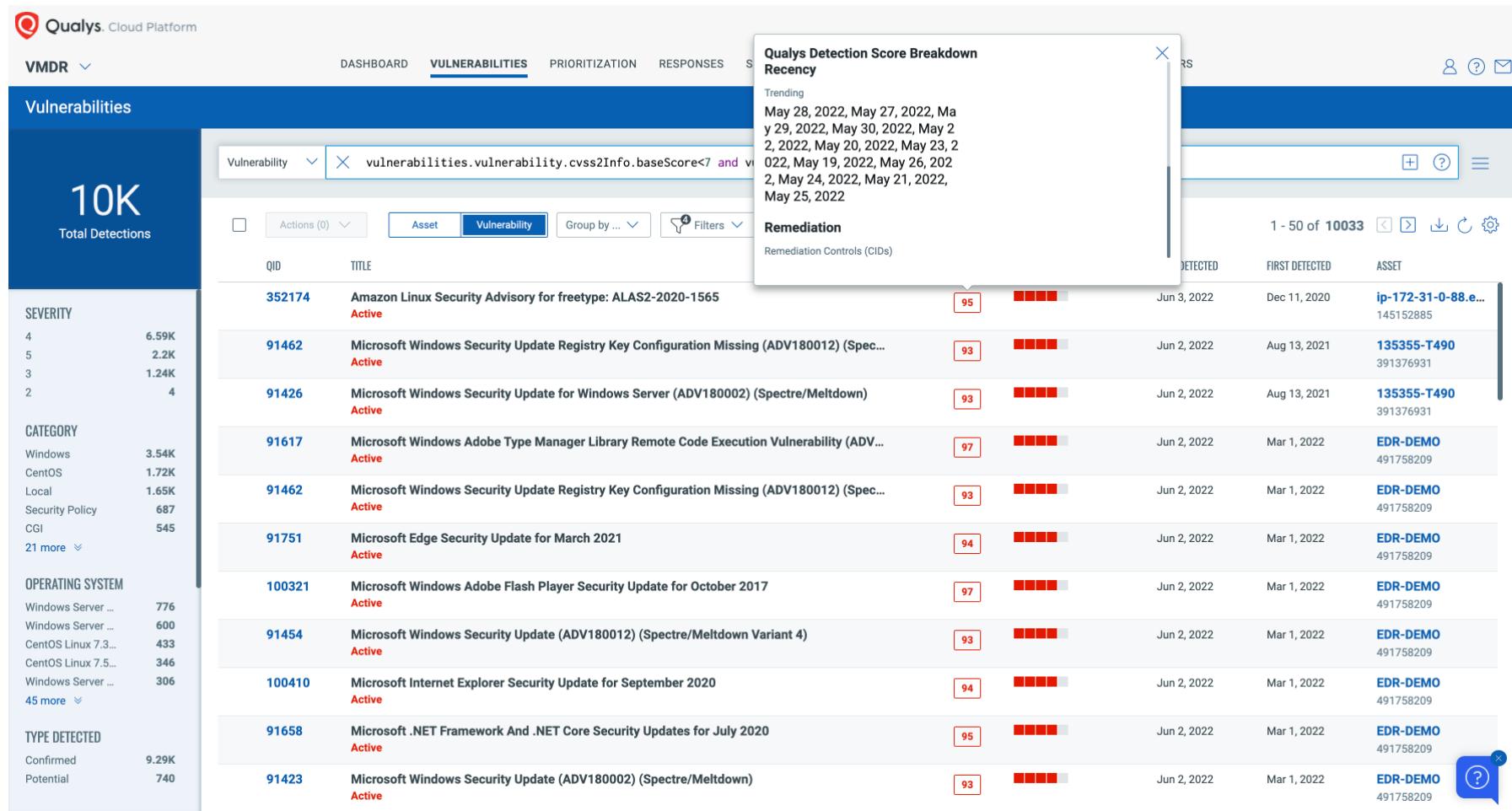
Here you can see that the vulnerability has been recently trending on social media and the dark web.



The screenshot shows the Qualys Cloud Platform interface. On the left, there's a sidebar with sections for 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), and TYPE DETECTED (Confirmed: 9.29K, Potential: 740). The main dashboard displays "10K Total Detections". The VULNERABILITIES tab is selected, showing a search bar with the query "vulnerabilities.vulnerability.cvss2Info.baseScore<7 and v...". A modal window titled "Qualys Detection Score Breakdown Recency" is open, showing a list of dates from May 28, 2022, to May 25, 2022. Below the modal is a table of vulnerabilities with columns: QID, TITLE, DETECTED, FIRST DETECTED, ASSET. The table lists several Microsoft Windows security updates, including ADV180012 and ADV180002, along with other advisories like ALAS2-2020-1565.

QID	TITLE	DETECTED	FIRST DETECTED	ASSET
352174	Amazon Linux Security Advisory for freetype: ALAS2-2020-1565 Active	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	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91426	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown) Active	Jun 2, 2022	Aug 13, 2021	135355-T490 391376931
91617	Microsoft Windows Adobe Type Manager Library Remote Code Execution Vulnerability (ADV... Active	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91462	Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spec... Active	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91751	Microsoft Edge Security Update for March 2021 Active	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
100321	Microsoft Windows Adobe Flash Player Security Update for October 2017 Active	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91454	Microsoft Windows Security Update (ADV180012) (Spectre/Meltdown Variant 4) Active	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
100410	Microsoft Internet Explorer Security Update for September 2020 Active	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91658	Microsoft .NET Framework And .NET Core Security Updates for July 2020 Active	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209
91423	Microsoft Windows Security Update (ADV180002) (Spectre/Meltdown) Active	Jun 2, 2022	Mar 1, 2022	EDR-DEMO 491758209

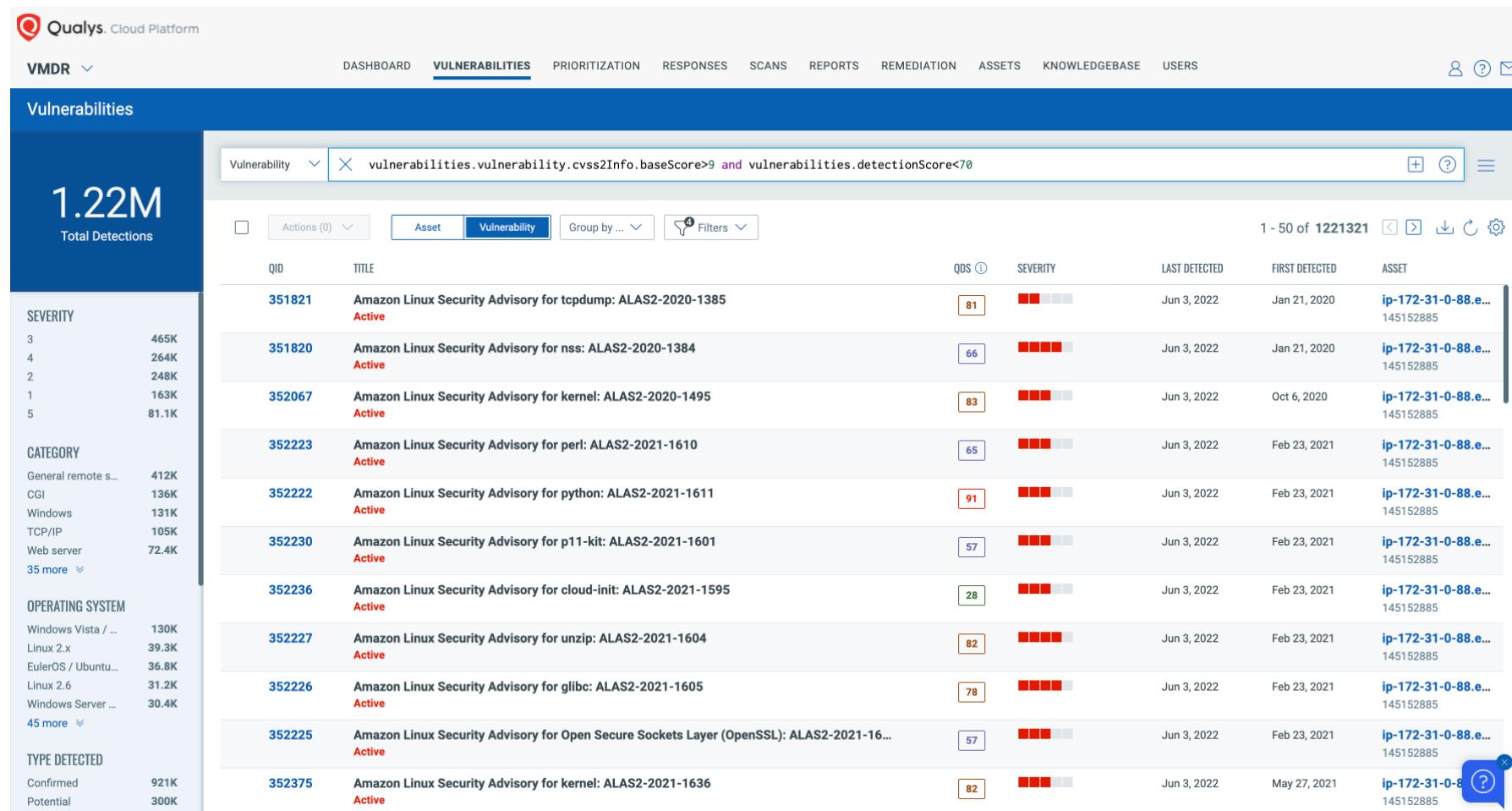
1 The exploit and trend dynamics of this Amazon Linux vulnerability reflect a high risk even though the CVSS score is in the Medium range.



The screenshot shows the Qualys Cloud Platform interface. The main dashboard displays "10K Total Detections". On the left, there are filters for "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), and "TYPE DETECTED" (Confirmed: 9.29K, Potential: 740). The central "VULNERABILITIES" tab is selected, showing a list of findings. A tooltip window titled "Qualys Detection Score Breakdown" provides details about the detection score breakdown for a specific entry (QID: 352174, Title: "Amazon Linux Security Advisory for freetype: ALAS2-2020-1565 Active"). The tooltip includes sections for "Trending" (listing dates from May 28, 2022, to May 25, 2022) and "Remediation" (listing remediation controls (CIDs)). The main list below the tooltip shows several other vulnerabilities, such as Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spec... Active) and Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown) Active.

QID	TITLE	Score	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
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

- 1 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.



The screenshot shows the Qualys Cloud Platform interface, specifically the Vulnerabilities section. The main header includes the Qualys logo, navigation tabs (VMDR, DASHBOARD, VULNERABILITIES, PRIORITIZATION, RESPONSES, SCANS, REPORTS, REMEDIATION, ASSETS, KNOWLEDGEBASE, USERS), and user icons. The VULNERABILITIES tab is selected.

A search bar at the top right contains the query: `vulnerabilities.vulnerability.cvss2Info.baseScore>9 and vulnerabilities.detectionScore<70`. Below the search bar are filter options: Actions (0), Asset (selected), Vulnerability, Group by ..., and Filters.

The main area displays a table of vulnerabilities with the following columns: QID, TITLE, QDS (Qualys Detection Score), SEVERITY, LAST DETECTED, FIRST DETECTED, and ASSET. The table lists 1221321 results, with the current view showing 1 - 50 of them.

On the left side, there are three vertical panels with summary data:

- SEVERITY:** 1.22M Total Detections, with counts for severity levels 3, 4, 2, 1, and 5.
- CATEGORY:** General remote s..., CGI, Windows, TCP/IP, Web server, and 35 more.
- OPERATING SYSTEM:** Windows Vista / ..., Linux 2.x, EulerOS / Ubuntu..., Linux 2.6, Windows Server ..., and 45 more.
- TYPE DETECTED:** Confirmed (921K) and Potential (300K).

- 1 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

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

Vulnerability ▾ X vulnerabilities.vulnerability.cvss2Info.baseScore>9 and vulnerabilities.detectionScore<70

Actions (0) Asset Vulnerability Group by ... Filters 1 - 50 of 1221321

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

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

The screenshot shows the Qualys Cloud Platform interface, specifically the Vulnerabilities section. A red box highlights the search bar containing the query: `vulnerabilities.vulnerability.cvss2Info.baseScore>9 and vulnerabilities.detectionScore<70`. The main table displays a list of vulnerabilities, each with columns for QID, Title, QDS (Qualys Detection Score), Severity, Last Detected, First Detected, and Asset. The first few rows are as follows:

QID	Title	QDS	Severity	Last Detected	First Detected	Asset
351821	Amazon Linux Security Advisory for tcpdump: ALAS2-2020-1385 <i>Active</i>	81	Medium	Jun 3, 2022	Jan 21, 2020	ip-172-31-0-88.e... 145152885
351820	Amazon Linux Security Advisory for nss: ALAS2-2020-1384 <i>Active</i>	66	Medium	Jun 3, 2022	Jan 21, 2020	ip-172-31-0-88.e... 145152885
352067	Amazon Linux Security Advisory for kernel: ALAS2-2020-1495 <i>Active</i>	83	Medium	Jun 3, 2022	Oct 6, 2020	ip-172-31-0-88.e... 145152885
352223	Amazon Linux Security Advisory for perl: ALAS2-2021-1610 <i>Active</i>	65	Medium	Jun 3, 2022	Feb 23, 2021	ip-172-31-0-88.e... 145152885
352222	Amazon Linux Security Advisory for python: ALAS2-2021-1611 <i>Active</i>	91	Medium	Jun 3, 2022	Feb 23, 2021	ip-172-31-0-88.e... 145152885
352230	Amazon Linux Security Advisory for p11-kit: ALAS2-2021-1601 <i>Active</i>	57	Medium	Jun 3, 2022	Feb 23, 2021	ip-172-31-0-88.e... 145152885
352236	Amazon Linux Security Advisory for cloud-init: ALAS2-2021-1595 <i>Active</i>	28	Medium	Jun 3, 2022	Feb 23, 2021	ip-172-31-0-88.e... 145152885
352227	Amazon Linux Security Advisory for unzip: ALAS2-2021-1604 <i>Active</i>	82	Medium	Jun 3, 2022	Feb 23, 2021	ip-172-31-0-88.e... 145152885
352226	Amazon Linux Security Advisory for glibc: ALAS2-2021-1605 <i>Active</i>	78	Medium	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... <i>Active</i>	57	Medium	Jun 3, 2022	Feb 23, 2021	ip-172-31-0-88.e... 145152885
352375	Amazon Linux Security Advisory for kernel: ALAS2-2021-1636 <i>Active</i>	82	Medium	Jun 3, 2022	May 27, 2021	ip-172-31-0-88.e... 145152885

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

Qualys. Cloud Platform

VMDR VULNERABILITIES PRIORITIZATION RESPONSES SCANS REPORTS REMEDIATION ASSETS KNOWLEDGEBASE USERS

**Vulnerabilities**

283 Total Detections

SEVERITY	193
4	193
5	70
3	13
2	6
1	1
CATEGORY	Windows 162
Local	53
Internet Explorer	26
Security Policy	19
Office Application	10
4 more	4 more
OPERATING SYSTEM	Windows Server ... 40
Windows Server ...	19
Windows Server ...	16
Windows Server ...	14
Windows Server ...	13
45 more	45 more
TYPE DETECTED	Confirmed 277
Potential	6

Vulnerability vulnerabilities.vulnerability.cvss2Info.baseScore>9 and vulnerabilities.detectionScore<70

Actions (0) Asset Vulnerability Group by ... Filters 1 - 50 of 283

QID	TITLE	QDS	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
124148	WinRAR SFX Module Remote Code Execution Vulnerability <span style="color: red;">Active</span>	77	9.3	2022 Mar 2, 2021	abc 313926894	
376538	Adobe Security Update for Adobe Acrobat and Adobe Reader (APSB22-16) <span style="color: red;">Active</span>	59	9.3	2022 Apr 20, 2022	abc 313926894	
90805	Microsoft Windows Unauthorized Digital Certificates Spoofing Vulnerability <span style="color: red;">Active</span>	77	9.3	2022 Aug 29, 2020	WIN-9JP58SDQS... 246504694	
90819	Microsoft Windows Unauthorized Digital Certificates Spoofing Vulnerability <span style="color: red;">Active</span>	77	9.3	2022 Aug 29, 2020	WIN-9JP58SDQS... 246504694	
124148	WinRAR SFX Module Remote Code Execution Vulnerability <span style="color: red;">Active</span>	77	9.3	2022 Nov 12, 2021	WIN7-30-114 432513403	
376538	Adobe Security Update for Adobe Acrobat and Adobe Reader (APSB22-16) <span style="color: red;">Active</span>	59	9.3	2022 Jun 2, 2022	WIN7-30-114 432513403	
100067	Microsoft Internet Explorer "Scripting.FileSystem" Security Bypass Vulnerability - Zero Day <span style="color: red;">Active</span>	67	9.3	2022 Aug 29, 2020	WIN2008DC.cisdi... 246230286	
118423	Hotfix KB2264107 (DLL hijacking) Not Installed / Not Configured <span style="color: red;">Active</span>	68	9.3	2022 Aug 29, 2020	WIN2008DC.cisdi... 246230286	
90949	Windows 8.1 and Windows Server 2012 R2 Update Missing (KB2919355) <span style="color: red;">Active</span>	64	9.3	2022 Jun 1, 2022	win-890lrmesc6 246207161	
90949	Windows 8.1 and Windows Server 2012 R2 Update Missing (KB2919355) <span style="color: red;">Active</span>	64	9.3	2022 Aug 29, 2020	win2012r2dc.disa... 246196129	
90949	Windows 8.1 and Windows Server 2012 R2 Update Missing (KB2919355) <span style="color: red;">Active</span>	64	9.3	2022 Aug 29, 2020	inbastion 246486231	

**Qualys Detection Score Breakdown**  
Highest contributing CVE to QDS:  
CVE-2022-28232 ...  
Attributes contributing to the CVSS score -  
**Technical Attributes**  
CVSS Score  
9.3  
**Remediation**  
Remediation Controls (CIDs)

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

Qualys, Cloud Platform

VMDR ▾ DASHBOARD VULNERABILITIES PRIORITIZATION RESPONSES SCANS REPORTS REMEDIATION ASSETS KNOWLEDGEBASE USERS

Vulnerabilities

283 Total Detections

SEVERITY: 4 (193), 5 (70), 3 (13), 2 (6), 1 (1)

CATEGORY: Windows (162), Local (53), Internet Explorer (26), Security Policy (19), Office Application (10), 4 more ▾

OPERATING SYSTEM: Windows Server ... (40), Windows Server ... (19), Windows Server ... (16), Windows Server ... (14), Windows Server ... (13), 45 more ▾

TYPE DETECTED: Confirmed (277), Potential (6)

Vulnerability ▾  Actions (0) Asset Vulnerability Group by ... Filters 1 - 50 of 283

QID	TITLE	QDS ⓘ	SEVERITY	LAST DETECTED	FIRST DETECTED	ASSET
124148	WinRAR SFX Module Remote Code Execution Vulnerability Active	59	CVSS Score: 9.3	Jun 2, 2022	Mar 2, 2021	abc 313926894
376538	Adobe Security Update for Adobe Acrobat and Adobe Reader (APSB22-16) Active	59	CVSS Score: 9.3	Jun 2, 2022	Apr 20, 2022	abc 313926894
90805	Microsoft Windows Unauthorized Digital Certificates Spoofing Vulnerability Active	64	CVSS Score: 9.3	Jun 1, 2022	Aug 29, 2020	WIN-9JP58SDQS... 246504694
90819	Microsoft Windows Unauthorized Digital Certificates Spoofing Vulnerability Active	67	CVSS Score: 9.3	Jun 2, 2022	Aug 29, 2020	WIN-9JP58SDQS... 246504694
124148	WinRAR SFX Module Remote Code Execution Vulnerability Active	64	CVSS Score: 9.3	Jun 2, 2022	Nov 12, 2021	WIN7-30-114 432513403
376538	Adobe Security Update for Adobe Acrobat and Adobe Reader (APSB22-16) Active	59	CVSS Score: 9.3	Jun 2, 2022	Apr 13, 2022	WIN7-30-114 432513403
100067	Microsoft Internet Explorer "Scripting.FileSystem" Security Bypass Vulnerability - Zero Day Active	67	CVSS Score: 9.3	Jun 2, 2022	Aug 29, 2020	WIN2008DC.cisdi... 246230286
118423	Hotfix KB2264107 (DLL hijacking) Not Installed / Not Configured Active	68	CVSS Score: 9.3	Jun 2, 2022	Aug 29, 2020	WIN2008DC.cisdi... 246230286
90949	Windows 8.1 and Windows Server 2012 R2 Update Missing (KB2919355) Active	64	CVSS Score: 9.3	Jun 1, 2022	Aug 29, 2020	win-890blrmsc6 246207161
90949	Windows 8.1 and Windows Server 2012 R2 Update Missing (KB2919355) Active	64	CVSS Score: 9.3	Jun 1, 2022	Aug 29, 2020	win2012r2dc.disa... 246196129
90949	Windows 8.1 and Windows Server 2012 R2 Update Missing (KB2919355) Active	64	CVSS Score: 9.3	Jun 1, 2022	Aug 29, 2020	inbastion 246486231

1 The previous examples were evaluating single vulnerabilities.

The screenshot shows the Qualys Cloud Platform interface, specifically the 'Vulnerabilities' section. On the left, there's a sidebar with various filters and statistics:

- Total Detections:** 1.22M
- TYPE DETECTED:**
  - Confirmed: 923K
  - Potential: 301K
- STATUS:**
  - NEW: 722K
  - ACTIVE: 494K
  - REOPENED: 8.09K
- CVSS RATING:**
  - MEDIUM: 531K
  - HIGH: 318K
  - Critical: 145K
  - LOW: 127K
  - NONE: 101K
- RTIS:**
  - Easy Exploit: 700K
  - Patch Not Available: 661K
  - Remote Code Exec.: 244K
  - Denial Of Service: 214K
  - High Data Loss: 208K
  - 13 more ...

The main content area displays a table of vulnerabilities with the following columns: QID, TITLE, QDS (Qualys Detection Score), SEVERITY, LAST DETECTED, FIRST DETECTED, and ASSET. The table lists several entries, such as TCP Sequence Number Approximation Based Denial of Service (QID 82054), Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher (QID 38601), and SSL Server May Be Forced to Use Weak Encryption Vulnerability (QID 38141). Each row includes a small icon indicating its status or type.

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

The screenshot shows the Qualys Cloud Platform interface, specifically the 'Vulnerabilities' section. The top navigation bar includes links for VMDR, DASHBOARD, VULNERABILITIES (which is underlined), PRIORITIZATION, RESPONSES, SCANS, REPORTS, REMEDIATION, ASSETS, KNOWLEDGEBASE, and USERS. On the left, there's a sidebar with metrics: 1.22M Total Detections, 45 more vulnerabilities, TYPE DETECTED (Confirmed: 923K, Potential: 301K), STATUS (NEW: 722K, ACTIVE: 494K, REOPENED: 8.09K), CVSS RATING (MEDIUM: 531K, HIGH: 318K, CRITICAL: 145K, LOW: 127K, NONE: 101K), and RTIS (Easy Exploit: 700K, Patch Not Available: 661K, Remote Code Exec.: 244K, Denial Of Service: 214K, High Data Loss: 208K). The main content area displays a table of vulnerabilities with columns: QID, TITLE, QDS (with a value of 83 highlighted in orange), SEVERITY (represented by a color-coded bar), LAST DETECTED, FIRST DETECTED, and ASSET (node-ecr.pool-1-1... 542910234). The table lists several entries, including TCP Sequence Number Approximation Based Denial of Service, Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher, SSL Server May Be Forced to Use Weak Encryption Vulnerability, and various jQuery and TLS related vulnerabilities. A blue callout bubble with a question mark icon is positioned over the last entry in the list.

Vulnerability	Search...					
Asset	Search...					
82054	TCP Sequence Number Approximation Based Denial of Service <b>New</b>	83	<span style="background-color: #ff0000; color: white; padding: 2px 5px;">83</span>	Jun 3, 2022	Jun 3, 2022	node-ecr.pool-1-1... 542910234
38601	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher ... <b>New</b>	33	<span style="background-color: #ff0000; color: white; padding: 2px 5px;">33</span>	Jun 3, 2022	Jun 3, 2022	node-ecr.pool-1-1... 542910234
38141	SSL Server May Be Forced to Use Weak Encryption Vulnerability <b>New</b>	24	<span style="background-color: #ff0000; color: white; padding: 2px 5px;">24</span>	Jun 3, 2022	Jun 3, 2022	node-ecr.pool-1-1... 542910234
13481	jQuery Prior to 3.4.0 Cross-Site Scripting Vulnerability <b>New</b>	34	<span style="background-color: #ffff00; color: black; padding: 2px 5px;">34</span>	Jun 3, 2022	Jun 3, 2022	node-ecr.pool-1-1... 542910234
11827	HTTP Security Header Not Detected <b>New</b>	15	<span style="background-color: #ff0000; color: white; padding: 2px 5px;">15</span>	Jun 3, 2022	Jun 3, 2022	node-ecr.pool-1-1... 542910234
38655	X.509 Certificate SHA1 Signature Collision Vulnerability <b>New</b>	16	<span style="background-color: #ff0000; color: white; padding: 2px 5px;">16</span>	Jun 3, 2022	Jun 3, 2022	node-ecr.pool-1-1... 542910234
38596	TLS Protocol Session Renegotiation Security Vulnerability <b>New</b>	85	<span style="background-color: #ffff00; color: black; padding: 2px 5px;">85</span>	Jun 3, 2022	Jun 3, 2022	node-ecr.pool-1-1... 542910234
13371	jQuery Prior to 1.9.0 Cross-Site Scripting Vulnerability <b>New</b>	85	<span style="background-color: #ffff00; color: black; padding: 2px 5px;">85</span>	Jun 3, 2022	Jun 3, 2022	node-ecr.pool-1-1... 542910234
13772	jQuery Cross-Site Scripting Vulnerability <b>New</b>	85	<span style="background-color: #ffff00; color: black; padding: 2px 5px;">85</span>	Jun 3, 2022	Jun 3, 2022	node-ecr.pool-1-1... 542910234
13481	jQuery Prior to 3.4.0 Cross-Site Scripting Vulnerability <b>New</b>	34	<span style="background-color: #ffff00; color: black; padding: 2px 5px;">34</span>	Jun 3, 2022	Jun 3, 2022	node-ecr.pool-1-1... 542910234
38606	SSL Server Has SSLv3 Enabled Vulnerability		<span style="background-color: #ff0000; color: white; padding: 2px 5px;">83</span>	Jun 3, 2022	Jun 3, 2022	node-ecr.pool-1-1...

1 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.

The screenshot shows the Qualys Cloud Platform interface for managing vulnerabilities. On the left, there's a sidebar with sections for Total Assets (123K), Software (Apache web server, gpg-pubkey, Windows Internet...), Hardware (Unidentified / Uni..., Computers / Uni..., Virtualized / Virtu...), and Manufacturer (Unidentified, VMware, Cisco Systems, MikroTik, HPE). The main area is titled 'Vulnerabilities' and displays a table of assets. The columns include NAME, CRITICALITY, RISK SCORE, OPERATING SYSTEM, LAST LOGGED IN, LAST SCANNED, SOURCES, and TAGS. A red box highlights the 'CRITICALITY' column, which contains values like 4, 2, and 1. The table lists various assets with their respective details, such as operating systems (Debian Project Debian Buster, SUSE Linux Enterprise Server 12, Amazon Web Services Amazon Linux 2, Canonical Ubuntu Xenial Xerus, Red Hat Enterprise Linux Server 6, Red Hat Enterprise Linux Server 7, Canonical Ubuntu Xenial Xerus), last logged in times, and last scanned times. There are also icons for AWS and Qualys sources, and various tags like 'No NetBIOS Name', 'FedRAMP', 'Operating System...', 'Scanned in 180-D', and 'OS: Ubuntu xx'.

NAME	CRITICALITY	RISK SCORE	OPERATING SYSTEM	LAST LOGGED IN	LAST SCANNED	SOURCES	TAGS
demo-gcp-uc1-debian-10-3.c.gcp-qualys-dem...	4	381	Debian Project Debian Buster 10.12	reboot	VM: 3 hours ago PC: 21 hours ago	Qualys AWS	No NetBIOS Name 24 more...
Demo-WU-WM06	4	727	SUSE Linux Enterprise Server 12.12 SP3	reboot	VM: an hour ago PC: 5 hours ago	Qualys AWS	FedRAMP 33 more...
ip-192-168-0-185.ec2.internal	4	721	Amazon Web Services Amazon Linux 2.0	reboot	VM: 27 minutes ago PC: 7 hours ago	Qualys AWS	Operating System... 17 more...
ip-172-31-0-45.eu-west-2.compute.internal	2	370	Canonical Ubuntu Xenial Xerus 16.04 LTS 16.04.6 LTS	reboot	VM: 4 hours ago PC: 9 hours ago	Qualys AWS	No NetBIOS Name 22 more...
demo-gcp-uw2-redhat-6-public-1.c.gcp-qualy...	4	739	Red Hat Enterprise Linux Server 6.10	reboot	VM: 11 hours ago PC: 7 hours ago	Qualys AWS	OS: RHEL Server 6.x 35 more...
ip-172-31-37-33.us-east-2.compute.internal	4	728	Red Hat Enterprise Linux Server 7.7	ec2-user	VM: 4 hours ago PC: 7 hours ago	Qualys AWS	Scanned in 180-D 33 more...
ip-192-168-0-38.ec2.internal	2	367	Canonical Ubuntu Xenial Xerus 16.04 LTS 16.04.6 LTS	reboot	VM: 4 hours ago PC: 13 hours ago	Qualys AWS	OS: Ubuntu xx 21 more...

1 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 screenshot shows the Qualys Cloud Platform interface. The top navigation bar includes VMDR, DASHBOARD, VULNERABILITIES (which is selected), PRIORITIZATION, RESPONSES, SCANS, REPORTS, REMEDIATION, ASSETS, KNOWLEDGEBASE, and USERS. A red box highlights the 'ASSET CRITICALITY SCORE' section in a modal window. The modal displays two scores: 3 and 4, with 4 being highlighted. Below the scores, it says 'Calculated as of Jun 3, 2022'. The main table lists various assets with their names, IP addresses, operating systems, last logged in status, last scanned time, sources, and tags. One asset, 'demo-gcp-uc1-debian-10-3.c.gcp-qualys-dem...', has a criticality score of 4 and is tagged as 'Data Center'.

NAME	IP ADDRESS	OS	LAST LOGGED IN	LAST SCANNED	SOURCES	TAGS
demo-gcp-uc1-debian-10-3.c.gcp-qualys-dem...	35.192.49.214, fe80:0:0:4001:aff:fe80:fe8, 10.128.15....	Debian Project Debian Buster 10.12	reboot	VM: 3 hours ago PC: 21 hours ago	aws	No NetBIOS Name Last Checked In a few seconds ago
Demo-WU-VM06	10.1.1.8, 40.112.175.189, fe80:0:0:20d:3aff:fe59:ffa9	SUSE Linux Enterprise Server 12.12 SP3	reboot	VM: an hour ago PC: 5 hours ago	aws	FedRAMP Last Checked In a few seconds ago
ip-192-168-0-185.ec2.internal	192.168.0.185	Amazon Web Services Amazon Linux 2.0	reboot	VM: 27 minutes ago PC: 7 hours ago	aws	Operating System ... Last Checked In a few seconds ago
ip-172-31-0-45.eu-west-2.compute.internal	172.31.0.45, 3.8.77.85	Canonical Ubuntu Xenial Xerus 16.04 LTS 16.04.6 LTS	reboot	VM: 4 hours ago PC: 9 hours ago	aws	No NetBIOS Name Last Checked In a few seconds ago
demo-gcp-uw2-redhat-6-public-1.c.gcp-qualy...	10.0.0.139, fe80:0:0:4001:aff:fe00:8b, 34.94.252.113	Red Hat Enterprise Linux Server 6.10	reboot	VM: 11 hours ago PC: 7 hours ago	aws	OS: RHEL Server 6.x Last Checked In a few seconds ago
ip-172-31-37-33.us-east-2.compute.internal	18.222.248.218, fe80:0:0:884:59ff:fe82:a3b0, 172.31....	Red Hat Enterprise Linux Server 7.7	ec2-user	VM: 4 hours ago PC: 7 hours ago	aws	Scanned in 180-D Last Checked In a few seconds ago
ip-192-168-0-38.ec2.internal	54.175.178.104, 192.168.0.38	Canonical Ubuntu Xenial Xerus 16.04 LTS 16.04.6 LTS	reboot	VM: 4 hours ago PC: 13 hours ago	aws	OS: Ubuntu xx Last Checked In a few seconds ago

1 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 screenshot shows the Qualys Cloud Platform interface with the 'VULNERABILITIES' tab selected. On the left, there's a summary section with '123K Total Assets' and breakdowns by category: SOFTWARE (Apache web server, gpg-pubkey, Windows Internet...), HARDWARE (Unidentified / Uni..., Computers / Uni..., Virtualized / Virtu...), and MANUFACTURER (Unidentified, VMware, Cisco Systems, MikroTik, HPE). The main area displays a table of vulnerabilities across multiple assets. The columns include NAME, CRITICALITY, RISK SCORE, OPERATING SYSTEM, LAST LOGGED IN, LAST SCANNED, SOURCES, and TAGS. The 'RISK SCORE' column is highlighted with a red border. The first asset listed is 'demo-gcp-uc1-debian-10-3.c.gcp-qualys-dem...' with a risk score of 381. Other assets shown include 'Demo-WU-VM06' (727), 'ip-192-168-0-185.ec2.internal' (721), 'ip-172-31-0-45.eu-west-2.compute.internal' (370), 'demo-gcp uw2-redhat-6-public-1.c.gcp-qualy...' (739), 'ip-172-31-37-33.us-east-2.compute.internal' (728), and 'ip-192-168-0-38.ec2.internal' (367).

NAME	CRITICALITY	RISK SCORE	OPERATING SYSTEM	LAST LOGGED IN	LAST SCANNED	SOURCES	TAGS
demo-gcp-uc1-debian-10-3.c.gcp-qualys-dem...	4	381	Debian Project Debian Buster 10.12	reboot	VM: 3 hours ago PC: 21 hours ago	aws	No NetBIOS Name 24 more...
Demo-WU-VM06	4	727	SUSE Linux Enterprise Server 12.12 SP3	reboot	VM: an hour ago PC: 5 hours ago	aws	FedRAMP 33 more...
ip-192-168-0-185.ec2.internal	4	721	Amazon Web Services Amazon Linux 2.2.0	reboot	VM: 27 minutes ago PC: 7 hours ago	aws	Operating System ... 17 more...
ip-172-31-0-45.eu-west-2.compute.internal	2	370	Canonical Ubuntu Xenial Xerus 16.04 LTS 16.04.6 LTS	reboot	VM: 4 hours ago PC: 9 hours ago	aws	No NetBIOS Name 22 more...
demo-gcp uw2-redhat-6-public-1.c.gcp-qualy...	4	739	Red Hat Enterprise Linux Server 6.10	reboot	VM: 11 hours ago PC: 7 hours ago	aws	OS: RHEL Server 6.x 35 more...
ip-172-31-37-33.us-east-2.compute.internal	4	728	Red Hat Enterprise Linux Server 7.7	ec2-user	VM: 4 hours ago PC: 7 hours ago	aws	Scanned in 180-D 33 more...
ip-192-168-0-38.ec2.internal	2	367	Canonical Ubuntu Xenial Xerus 16.04 LTS 16.04.6 LTS	reboot	VM: 4 hours ago PC: 13 hours ago	aws	OS: Ubuntu xx 21 more...

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

The screenshot shows the Qualys Cloud Platform interface, specifically the Vulnerabilities section. On the left, a sidebar displays '123K Total Assets' categorized by type: SOFTWARE, HARDWARE, and MANUFACTURER. The main area lists vulnerabilities across various assets. A specific asset, 'ip-172-31-37-33.us-east-2.compute.internal', has its Risk Score (728) highlighted with a red box. The table columns include NAME, CRITICALITY, RISK SCORE, OPERATING SYSTEM, LAST LOGGED IN, LAST SCANNED, SOURCES, and TAGS. Each row provides detailed information about the asset's configuration and status.

NAME	CRITICALITY	RISK SCORE	OPERATING SYSTEM	LAST LOGGED IN	LAST SCANNED	SOURCES	TAGS
demo-gcp-uw2-redhat-6-public-1.c.gcp-qualy... 10.0.0.139, fe80:0:0:4001:aff:fe00:8b, 34.94.252.113	4	739	Red Hat Enterprise Linux Server 6 6.10	reboot	VM: 11 hours ago PC: 7 hours ago	aws	OS: RHEL Server 6.x Last Checked In a few seconds ago 21 more...
ip-172-31-37-33.us-east-2.compute.internal 18.222.248.218, fe80:0:0:884:59ff:fe82:a3b0, 172.31....	4	728	Red Hat Enterprise Linux Server 7 7.7	ec2-user	VM: 4 hours ago PC: 7 hours ago	aws	Scanned in 180-D Last Checked In a few seconds ago 33 more...
demo-gcp-uc1-vm1.c.gcp-quals-demo.internal 35.232.131.27, fe80:0:0:4001:aff:fe80:fea, 10.128.15....	4	719	Debian Project Debian GNU/Linux Buster 10.2	reboot	VM: 6 hours ago PC: 2 days ago	aws	All Assets Last Checked In a few seconds ago 16 more...
qualys-demo-instances-uscentral1.c.qualys-d... 10.128.0.9, fe80:0:0:4001:aff:fe80:9, 35.224.95.189	4	727	Red Hat Enterprise Linux Server 7 7.8	reboot	VM: an hour ago PC: 13 hours ago	aws	Data Center Last Checked In a few seconds ago 33 more...
ip-192-168-0-38.ec2.internal 54.175.178.104, 192.168.0.38	2	367	Canonical Ubuntu Xenial Xerus 16.04 LTS 16.04.6 LTS	reboot	VM: 4 hours ago PC: 14 hours ago	aws	OS: Ubuntu xx Last Checked In a few seconds ago 21 more...
demo-gcp-ue1-ubuntu-16-public-1.c.gcp-qual... 10.0.0.19, fe80:0:0:4001:aff:fe00:13, 35.231.248.26	4	742	Debian Project Debian Stretch 9.8	reboot	VM: 3 hours ago PC: a day ago	aws	GCP Asset Last Checked In a few seconds ago 17 more...
ip-172-31-0-88.eu-west-2.compute.internal 172.31.0.88	4	723	Amazon Web Services Amazon Linux 2 2.0	reboot	VM: 5 hours ago PC: 9 hours ago	aws	No Asset Group Last Checked In a few seconds ago 18 more...

- 1 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 screenshot shows the Qualys Cloud Platform interface. The top navigation bar includes links for VMDR, DASHBOARD, VULNERABILITIES (which is currently selected), PRIORITIZATION, RESPONSES, SCANS, REPORTS, REMEDIATION, ASSETS, KNOWLEDGEBASE, and USERS. The main content area displays a list of vulnerabilities across various assets, including their names, severities, and risk scores. A modal window is open in the center, titled "Asset Risk Score (ARS) Calculations". It contains the following information:

**Asset Risk Score is derived from the criticality of the asset, weighted average of vulnerabilities.**

**Contributing Factors**  
Asset Criticality Tag (Highest contributor)

Data Center ..... 4

Vulnerabilities

Critical.....12	High.....46	Medium.....27	Low.....14
-----------------	-------------	---------------	------------

**Formula for ARS:**

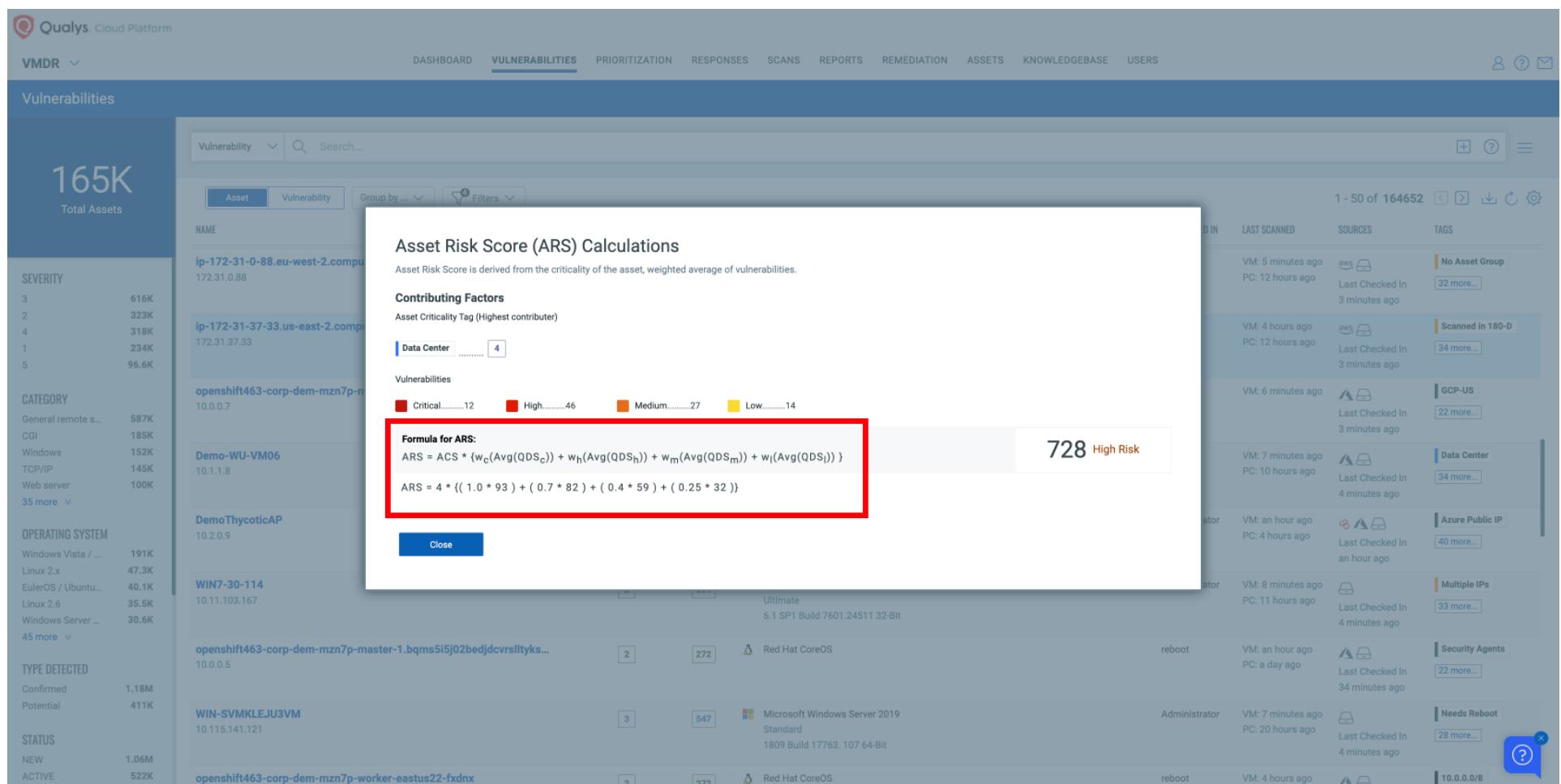
$$ARS = ACS * \{w_c(Avg(QDS_c)) + w_h(Avg(QDS_h)) + w_m(Avg(QDS_m)) + w_l(Avg(QDS_l))\}$$

$$ARS = 4 * ((1.0 * 93) + (0.7 * 82) + (0.4 * 59) + (0.25 * 32))$$

**Result:** 728 High Risk

The "728 High Risk" result is highlighted with a red box. The background of the main interface shows a list of assets with their last scanned times, sources, and tags. One asset, "WIN7-30-114", is shown with its operating system details: Ultimate 6.1 SP1 Build 7601.24511 32-BIT.

- 1 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 screenshot shows the Qualys Cloud Platform interface with the 'VULNERABILITIES' tab selected. A modal dialog box is open, titled 'Asset Risk Score (ARS) Calculations'. Inside the dialog, it states: 'Asset Risk Score is derived from the criticality of the asset, weighted average of vulnerabilities.' Below this, under 'Contributing Factors', it says 'Asset Criticality Tag (Highest contributor)'. It lists four categories: Data Center (4), Vulnerabilities (12 Critical, 46 High, 27 Medium, 14 Low), Demo-WU-VM06 (10.1.1.8), and DemoThycoticAP (10.2.0.9). The formula for ARS is displayed:

$$ARS = ACS * \{w_c(Avg(QDS_c)) + w_h(Avg(QDS_h)) + w_m(Avg(QDS_m)) + w_l(Avg(QDS_l))\}$$

$$ARS = 4 * ((1.0 * 93) + (0.7 * 82) + (0.4 * 59) + (0.25 * 32))$$

The calculated result is **728 High Risk**. The entire formula section is highlighted with a red border.

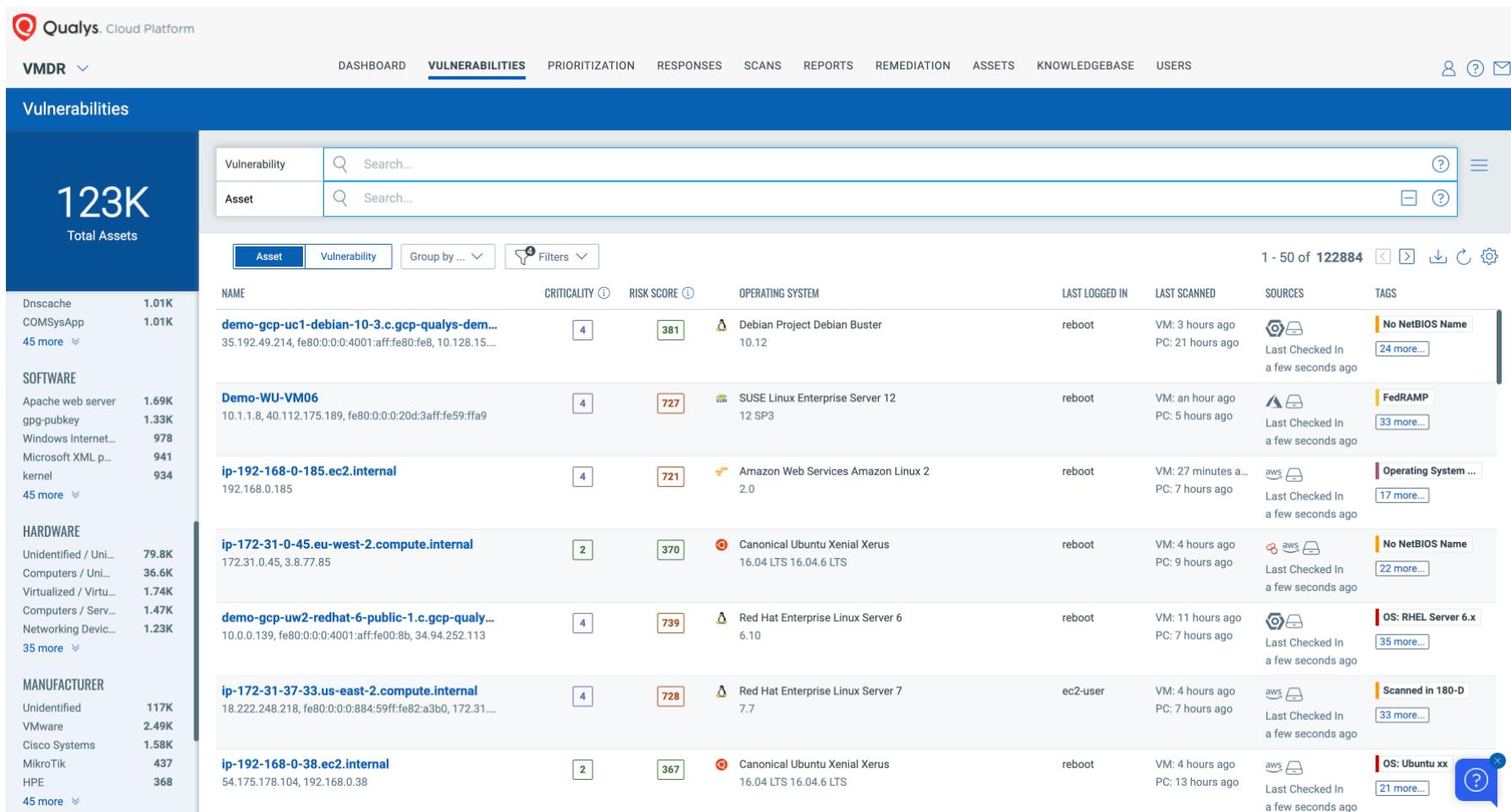
1 The steps to follow presents a use case to query a specific set of assets.

The screenshot shows the Qualys Cloud Platform interface, specifically the Vulnerabilities section. On the left, there's a sidebar with asset counts: 123K Total Assets, 1.01K Dnscache, 1.01K COMSysApp, 45 more under SOFTWARE; 1.69K Apache web server, 1.33K gpg-pubkey, 978 Windows Internet..., 941 Microsoft XML p..., 934 kernel under SOFTWARE; 79.8K Unidentified / Uni..., 36.6K Computers / Uni..., 1.74K Virtualized / Virtu..., 1.47K Computers / Serv..., 1.23K Networking Devic... under HARDWARE; 117K Unidentified, 2.49K VMware, 1.58K Cisco Systems, 437 MikroTik, 368 HPE, 45 more under MANUFACTURER.

The main content area displays a table of vulnerabilities. The columns include: NAME, CRITICALITY, RISK SCORE, OPERATING SYSTEM, LAST LOGGED IN, LAST SCANNED, SOURCES, and TAGS. The first few rows shown are:

- demo-gcp-uc1-debian-10-3.c.gcp-qualys-dem... (Criticality 4, Risk Score 381, Debian Project Debian Buster 10.12, reboot, VM: 3 hours ago, PC: 21 hours ago, Last Checked In a few seconds ago, No NetBIOS Name, 24 more...)
- Demo-WU-VM06 (Criticality 4, Risk Score 727, SUSE Linux Enterprise Server 12 12 SP3, reboot, VM: an hour ago, PC: 5 hours ago, Last Checked In a few seconds ago, FedRAMP, 33 more...)
- ip-192-168-0-185.ec2.internal (Criticality 4, Risk Score 721, Amazon Web Services Amazon Linux 2 2.0, reboot, VM: 27 minutes ago, PC: 7 hours ago, aws, Last Checked In a few seconds ago, Operating System..., 17 more...)
- ip-172-31-0-45.eu-west-2.compute.internal (Criticality 2, Risk Score 370, Canonical Ubuntu Xenial Xerus 16.04 LTS 16.04.6 LTS, reboot, VM: 4 hours ago, PC: 9 hours ago, aws, Last Checked In a few seconds ago, No NetBIOS Name, 22 more...)
- demo-gcp-uw2-redhat-6-public-1.c.gcp-qualy... (Criticality 4, Risk Score 739, Red Hat Enterprise Linux Server 6 6.10, reboot, VM: 11 hours ago, PC: 7 hours ago, Last Checked In a few seconds ago, OS: RHEL Server 6.x, 35 more...)
- ip-172-31-37-33.us-east-2.compute.internal (Criticality 4, Risk Score 728, Red Hat Enterprise Linux Server 7 7.7, ec2-user, VM: 4 hours ago, PC: 7 hours ago, aws, Last Checked In a few seconds ago, Scanned in 180-D, 33 more...)
- ip-192-168-0-38.ec2.internal (Criticality 2, Risk Score 367, Canonical Ubuntu Xenial Xerus 16.04 LTS 16.04.6 LTS, reboot, VM: 4 hours ago, PC: 13 hours ago, aws, Last Checked In a few seconds ago, OS: Ubuntu xx, 21 more...)

1 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.

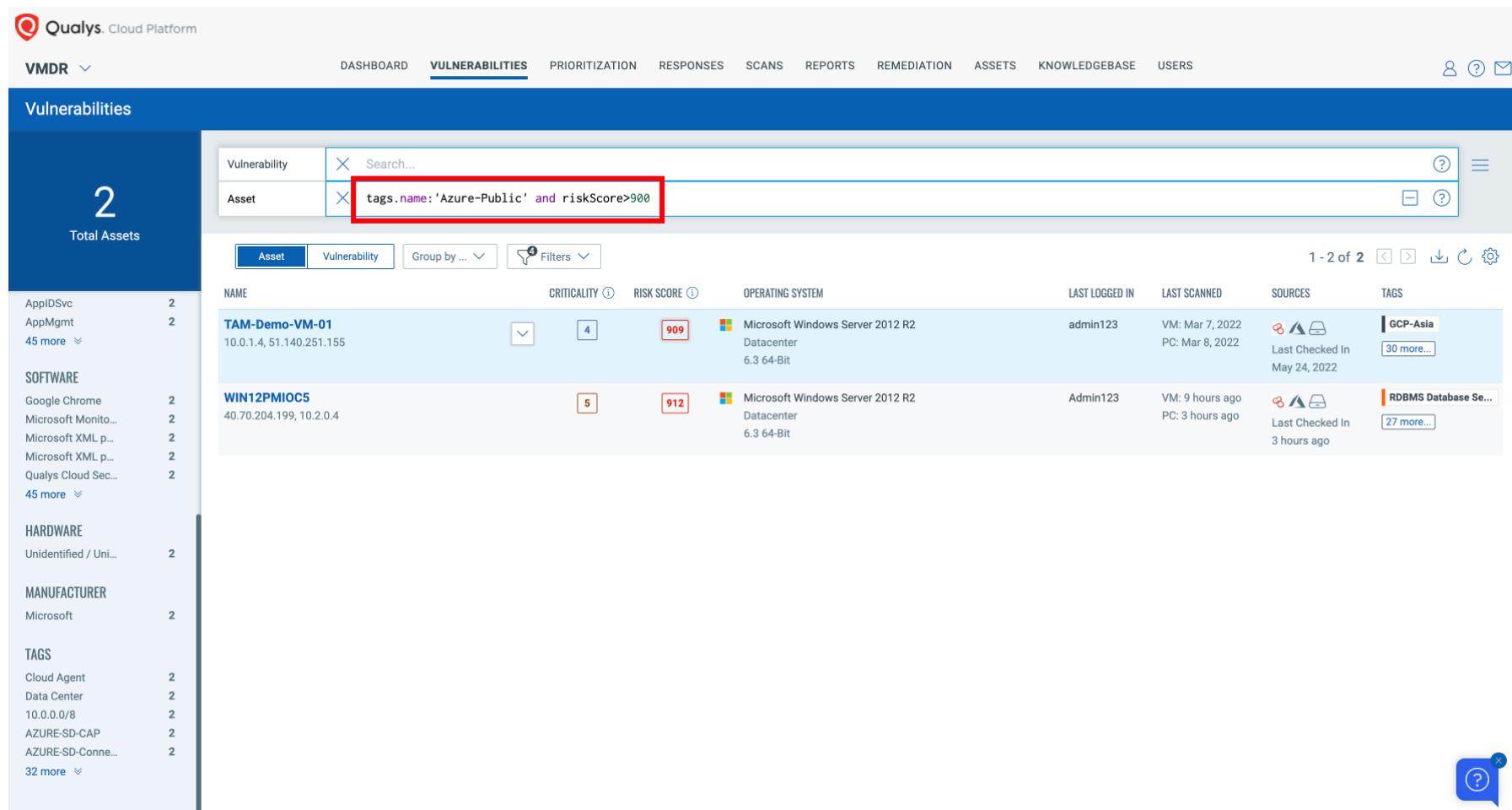


The screenshot shows the Qualys Cloud Platform VMDR interface under the 'VULNERABILITIES' tab. A large blue banner at the top displays '123K Total Assets'. Below this, there are two search bars: one for 'Vulnerability' and one for 'Asset', both with placeholder text 'Search...'. The main table lists vulnerabilities across different asset types:

NAME	Criticality	Risk Score	OPERATING SYSTEM	LAST LOGGED IN	LAST SCANNED	SOURCES	TAGS
demo-gcp-uc1-debian-10-3.c.gcp-qualys-dem...	4	381	Debian Project Debian Buster 10.12	reboot	VM: 3 hours ago PC: 21 hours ago	aws	No NetBIOS Name Last Checked In a few seconds ago 24 more...
Demo-WU-VM06	4	727	SUSE Linux Enterprise Server 12.12 SP3	reboot	VM: an hour ago PC: 5 hours ago	aws	FedRAMP Last Checked In a few seconds ago 33 more...
ip-192-168-0-185.ec2.internal	4	721	Amazon Web Services Amazon Linux 2.0	reboot	VM: 27 minutes ago PC: 7 hours ago	aws	Operating System ... Last Checked In a few seconds ago 17 more...
ip-172-31-0-45.eu-west-2.compute.internal	2	370	Canonical Ubuntu Xenial Xerus 16.04 LTS 16.04.6 LTS	reboot	VM: 4 hours ago PC: 9 hours ago	aws	No NetBIOS Name Last Checked In a few seconds ago 22 more...
demo-gcp-uw2-redhat-6-public-1.c.gcp-qualy...	4	739	Red Hat Enterprise Linux Server 6.10	reboot	VM: 11 hours ago PC: 7 hours ago	aws	OS: RHEL Server 6.x Last Checked In a few seconds ago 35 more...
ip-172-31-37-33.us-east-2.compute.internal	4	728	Red Hat Enterprise Linux Server 7.7	ec2-user	VM: 4 hours ago PC: 7 hours ago	aws	Scanned in 180-D Last Checked In a few seconds ago 33 more...
ip-192-168-0-38.ec2.internal	2	367	Canonical Ubuntu Xenial Xerus 16.04 LTS 16.04.6 LTS	reboot	VM: 4 hours ago PC: 13 hours ago	aws	OS: Ubuntu xx Last Checked In a few seconds ago 21 more...

1

Here you see the query to produce our dataset.



The screenshot shows the Qualys Cloud Platform interface, specifically the Vulnerabilities section. On the left, there's a sidebar with asset counts: 2 Total Assets, 45 more under SOFTWARE, 4 more under HARDWARE, 2 under MANUFACTURER, and 32 more under TAGS. The main area displays a table of vulnerabilities. At the top of the table, there's a search bar and a filter bar. The filter bar has an 'Asset' dropdown and a text input field containing the query: `tags.name:'Azure-Public' and riskScore>900`. This query filters the results to show two specific assets: 'TAM-Demo-VM-01' and 'WIN12PMIOCS'. Both assets have a risk score of 909 and 912 respectively. The table includes columns for NAME, CRITICALITY, RISK SCORE, OPERATING SYSTEM, LAST LOGGED IN, LAST SCANNED, SOURCES, and TAGS. The SOURCES column shows monitoring sources like GCP-Asia and RDBMS Database Server. The TAGS column lists Azure tags like AZURE-SD-CAP and AZURE-SD-Conne...

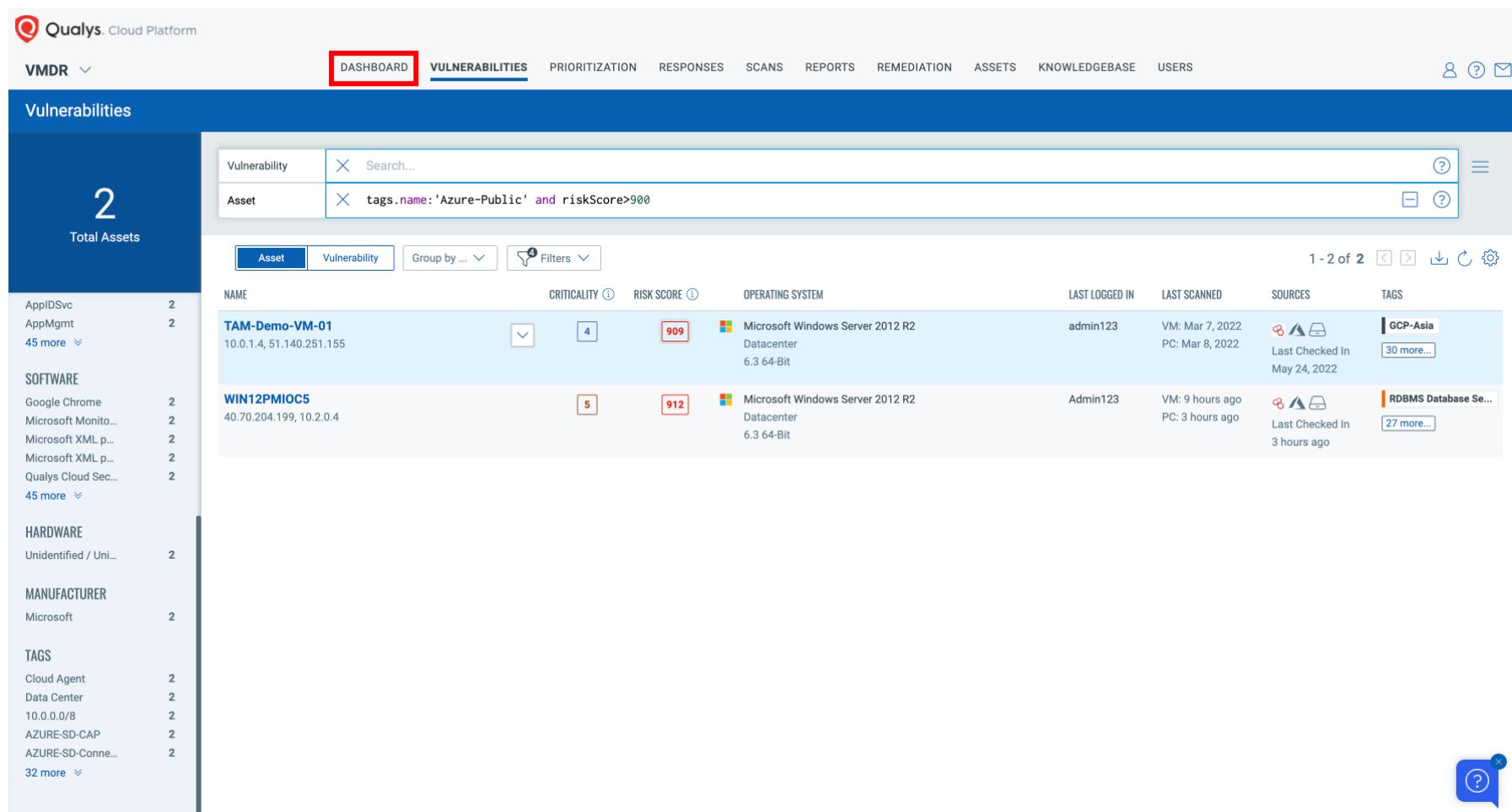
NAME	CRITICALITY	RISK SCORE	OPERATING SYSTEM	LAST LOGGED IN	LAST SCANNED	SOURCES	TAGS
TAM-Demo-VM-01 10.0.1.4, 51.140.251.155	4	909	Microsoft Windows Server 2012 R2 Datacenter 6.3 64-Bit	admin123	VM: Mar 7, 2022 PC: Mar 8, 2022	GCP-Asia Last Checked In May 24, 2022	30 more...
WIN12PMIOCS 40.70.204.199, 10.2.0.4	5	912	Microsoft Windows Server 2012 R2 Datacenter 6.3 64-Bit	Admin123	VM: 9 hours ago PC: 3 hours ago	RDBMS Database Server Last Checked In 3 hours ago	27 more...

- 1 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.

The screenshot shows the Qualys Cloud Platform interface, specifically the Vulnerabilities section. The top navigation bar includes links for DASHBOARD, VULNERABILITIES (which is underlined), PRIORITIZATION, RESPONSES, SCANS, REPORTS, REMEDIATION, ASSETS, KNOWLEDGEBASE, and USERS. On the left sidebar, there are sections for Total Assets (2), SOFTWARE (AppIDSvc, AppMgmt, 45 more), and HARDWARE (Unidentified / Uni...). The main content area displays a table of vulnerabilities. A search bar at the top right allows filtering by Asset or Vulnerability, with the current filter being "tags.name:'Azure-Public' and riskScore>900". The table columns include NAME, CRITICALITY (with a dropdown showing 4 for TAM-Demo-VM-01 and 5 for WIN12PMIOCS), RISK SCORE (highlighted with red boxes containing 909 and 912), OPERATING SYSTEM (Microsoft Windows Server 2012 R2 Datacenter 6.3 64-Bit for both), LAST LOGGED IN (admin123 for TAM-Demo-VM-01, Admin123 for WIN12PMIOCS), LAST SCANNED (VM: Mar 7, 2022, PC: Mar 8, 2022 for TAM-Demo-VM-01; VM: 9 hours ago, PC: 3 hours ago for WIN12PMIOCS), SOURCES (Last Checked In May 24, 2022 for TAM-Demo-VM-01; Last Checked In 3 hours ago for WIN12PMIOCS), and TAGS (GCP-Asia for TAM-Demo-VM-01; RDBMS Database Se... for WIN12PMIOCS). A blue question mark icon is located in the bottom right corner of the page.

NAME	CRITICALITY	RISK SCORE	OPERATING SYSTEM	LAST LOGGED IN	LAST SCANNED	SOURCES	TAGS
TAM-Demo-VM-01 10.0.1.4, 51.140.251.155	4	909	Microsoft Windows Server 2012 R2 Datacenter 6.3 64-Bit	admin123	VM: Mar 7, 2022 PC: Mar 8, 2022	Last Checked In May 24, 2022	GCP-Asia 30 more...
WIN12PMIOCS 40.70.204.199, 10.2.0.4	5	912	Microsoft Windows Server 2012 R2 Datacenter 6.3 64-Bit	Admin123	VM: 9 hours ago PC: 3 hours ago	Last Checked In 3 hours ago	RDBMS Database Se... 27 more...

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



The screenshot shows the Qualys Cloud Platform interface, specifically the Vulnerabilities section. A red box highlights the 'DASHBOARD' tab in the top navigation bar. The main view displays a table of assets, with two entries visible:

NAME	Criticality	Risk Score	Operating System	Last Logged In	Last Scanned	Sources	Tags
TAM-Demo-VM-01 10.0.1.4, 51.140.251.155	4	909	Microsoft Windows Server 2012 R2 Datacenter 6.3 64-Bit	admin123	VM: Mar 7, 2022 PC: Mar 8, 2022	 	GCP-Asia Last Checked In May 24, 2022 30 more...
WIN12PMIOCS 40.70.204.199, 10.2.0.4	5	912	Microsoft Windows Server 2012 R2 Datacenter 6.3 64-Bit	Admin123	VM: 9 hours ago PC: 3 hours ago	 	RDBMS Database Se... Last Checked In 3 hours ago 27 more...

On the left sidebar, there are filters for Asset Type (Asset, Vulnerability), Group by..., and Filters. The sidebar also lists categories like Software, Hardware, Manufacturer, and Tags, each with a count of 2 assets.

**1** Click Dashboard.

The screenshot shows the Qualys Cloud Platform interface. The top navigation bar includes VMDR, DASHBOARD, VULNERABILITIES (which is selected), PRIORITIZATION, RESPONSES, SCANS, REPORTS, REMEDIATION, ASSETS, KNOWLEDGEBASE, and USERS. The user profile icon is in the top right corner.

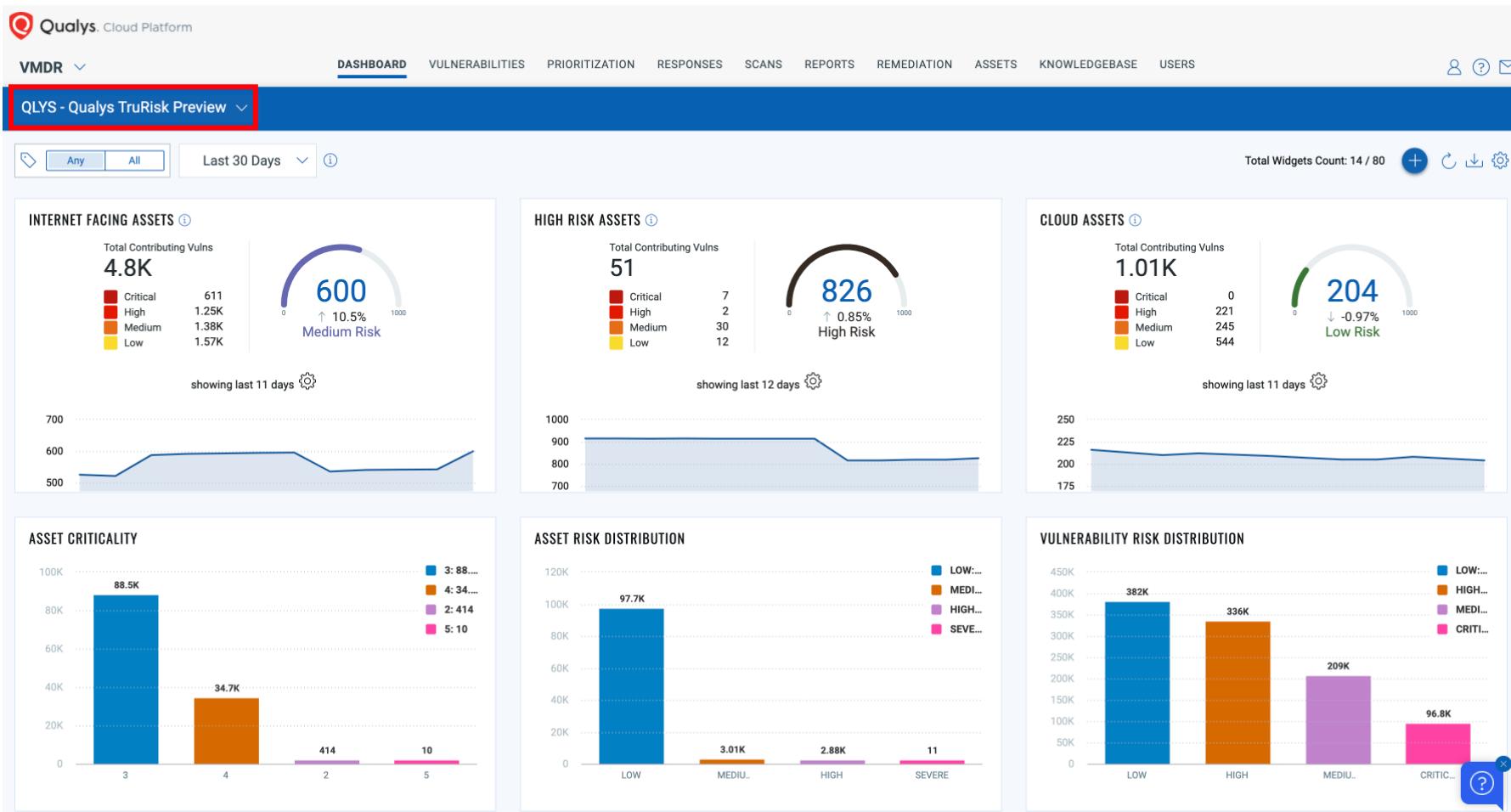
The main content area is titled "Vulnerabilities". On the left, there's a sidebar with "Total Assets" (2) and lists for SOFTWARE, HARDWARE, MANUFACTURER, and TAGS. The SOFTWARE section lists AppIDSvc, AppMgmt, and 45 more. The HARDWARE section lists Unidentified / Uni... (2). The MANUFACTURER section lists Microsoft (2). The TAGS section lists Cloud Agent, Data Center, 10.0.0.0/8, AZURE-SD-CAP, AZURE-SD-Conne..., and 32 more.

The central part of the screen displays a table of vulnerabilities. The table has columns: NAME, CRITICALITY, RISK SCORE, OPERATING SYSTEM, LAST LOGGED IN, LAST SCANNED, SOURCES, and TAGS. There are two rows in the table:

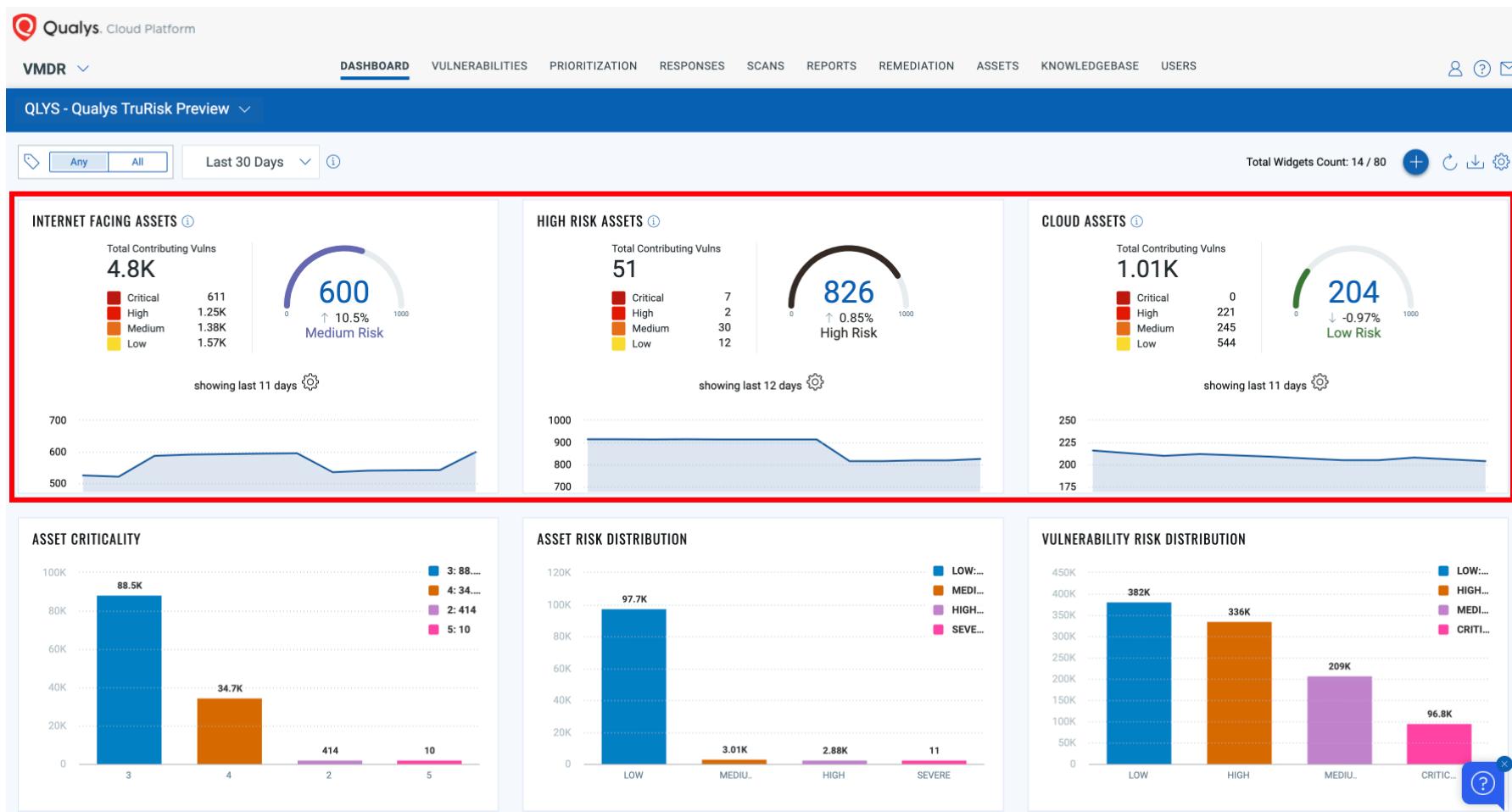
NAME	CRITICALITY	RISK SCORE	OPERATING SYSTEM	LAST LOGGED IN	LAST SCANNED	SOURCES	TAGS
TAM-Demo-VM-01 10.0.1.4, 51.140.251.155	4	909	Microsoft Windows Server 2012 R2 Datacenter 6.3 64-Bit	admin123	VM: Mar 7, 2022 PC: Mar 8, 2022		GCP-Asia Last Checked In May 24, 2022 30 more...
WIN12PMIOCS 40.70.204.199, 10.2.0.4	5	912	Microsoft Windows Server 2012 R2 Datacenter 6.3 64-Bit	Admin123	VM: 9 hours ago PC: 3 hours ago		RDBMS Database Se... Last Checked In 3 hours ago 27 more...

At the bottom right of the dashboard is a blue speech bubble icon with a question mark inside.

- 1 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.

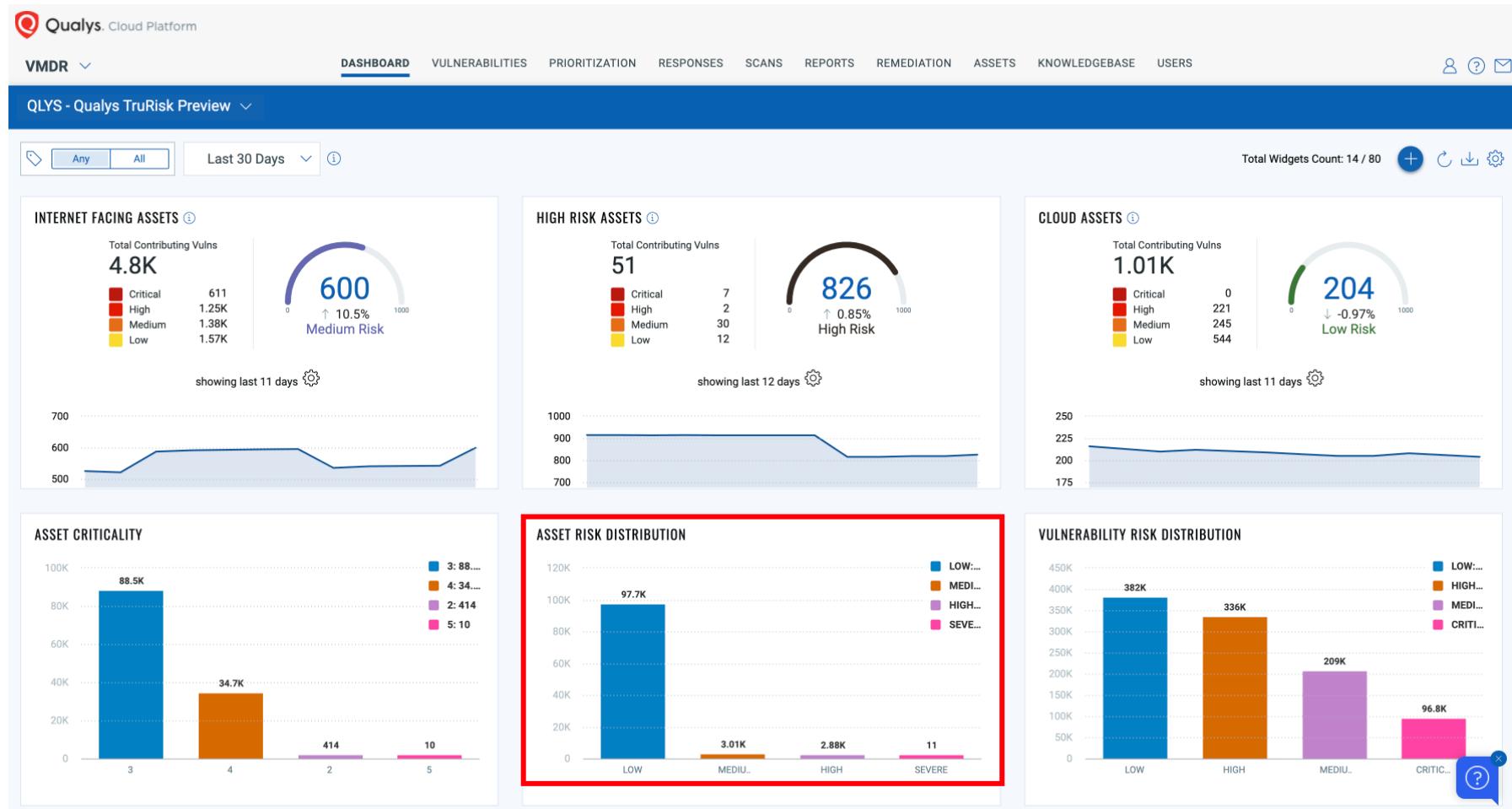


1 You can create many different widgets to visually monitor. Here you see widgets monitoring Risk Scores for Internet-facing assets, high risk assets, and cloud assets.



- 1 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.

# biorad | Qualys TruRisk Scoring



1

That's it. You're done.

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	High	Medium	Low
611	1.25K	1.38K	1.57K

600 ↑ 10.5% Medium Risk

Showing last 11 days ⓘ

**HIGH RISK ASSETS ⓘ**

Total Contributing Vulns: 51

Critical	High	Medium	Low
7	2	30	12

826 ↑ 0.85% High Risk

Showing last 12 days ⓘ

**CLOUD ASSETS ⓘ**

Total Contributing Vulns: 1.01K

Critical	High	Medium	Low
0	221	245	544

204 ↓ -0.97% Low Risk

Showing last 11 days ⓘ

**ASSET CRITICALITY**

3: 88.5K, 4: 34.7K, 2: 414, 5: 10

**ASSET RISK DISTRIBUTION**

LOW: 97.7K, MEDIUM: 3.01K, HIGH: 2.88K, SEVERE: 11

**VULNERABILITY RISK DISTRIBUTION**

LOW: 382K, HIGH: 336K, MEDIUM: 209K, CRITICAL: 96.8K



Scan to go to the interactive player