Qualys Cloud Platform v3.x

Unified Dashboard 1.0

Release Notes

Version 3.11.1
May 9, 2022

Here's what's new in Qualys Cloud Suite 3.11.1!

UD Unified Dashboard

VMDR Vulnerability Management, Detection, and Response

New Function Type to calculate Fixed Vulnerabilities

Unique Vulnerability Count to calculate Unique Vulnerabilities

Columns to Display option for the Title Group By

New Tokens Support

Qualys Cloud Platform 3.11.1 brings you many more improvements and updates! Learn more

New Function Type to Calculate Fixed Vulnerabilities

We have added a Function Type **Average** to calculate the **Fixed Age (MTTR)** of the Fixed vulnerabilities. This function Type is available in the **Numerical** Widget.

The Mean Time To Remediate (MTTR) is the average for the number of days it took to fix the vulnerability. The value of MTTR is generated in hours, days, months, and years.

The MTTR is calculated using the following formula:

Time of Remediation (ToR) - Time of Detection (ToD) = Time of Risk Exposure (ToRE)

MTTR = Time of Risk Exposure (ToRE) / Number of vulnerabilities found

Example:

Average time to remediate vulnerabilities from the duration October 14, 2019, to December 1, 2019:

Duration**:** 48 days (it does not include the end date of the duration.)

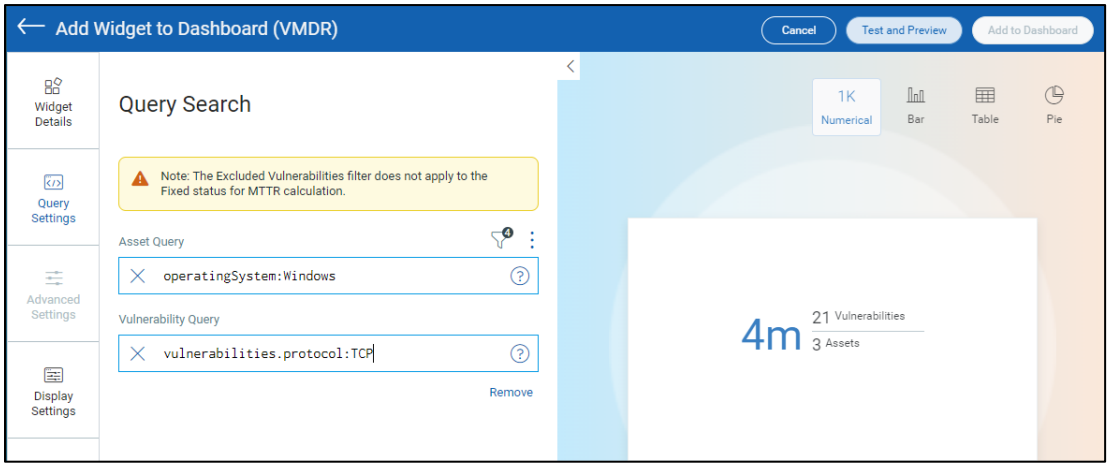
Number of vulnerabilities found = 30

Thus, applying the given data to the formula:

October 14, 2019 - December 1, 2019 = 1,152 hours (ToRE)

MTTR = 1152 (ToRE) / 30 (Number of vulnerabilities found) = 38.4 hours. = 2 days

To calculate MTTR, go to the **VMDR** dashboard > **Widget Details**, and in the **Function Type**, choose **Average**. In the **Select Field,** the **Fixed Age (MTTR)** is the only field and is selected by default.



In the **Query Settings**, add an **Asset Query** and **Vulnerability Query** to determine the average number of days it took to fix the vulnerabilities associated with the assets.

Unique Vulnerability Count to Calculate Unique Vulnerabilities

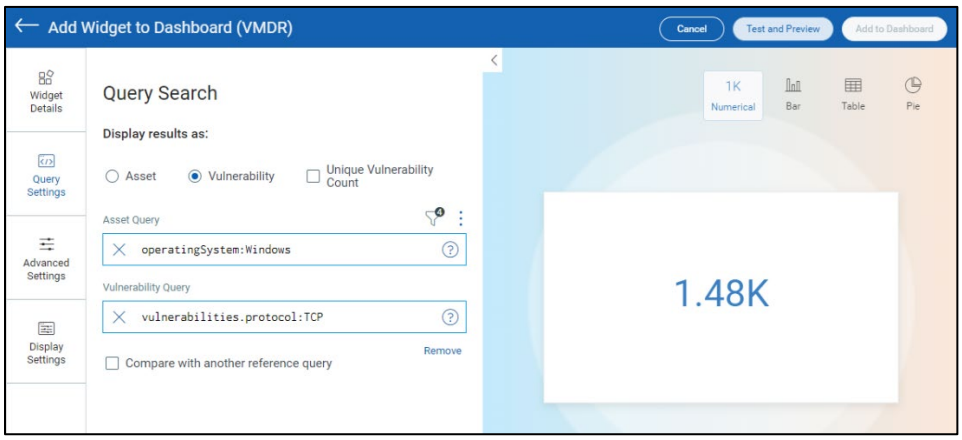
Previously, when calculating the vulnerability count, in a count widget, the count included the same vulnerability on different assets. Thus, the same vulnerability was calculated twice causing duplication in the data. We have now introduced a new option **Unique Vulnerability Count** that calculates the unique vulnerabilities on different assets.

The Unique Vulnerability Count is available for **Vulnerability Management** and **Threat Protection** application.

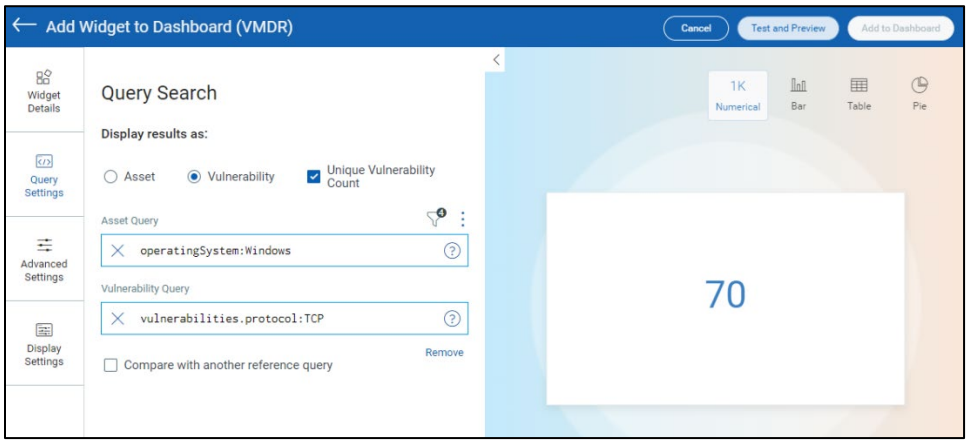
To select the Unique Vulnerability Count, in the **VMDR** dashboard > **Query Settings** > **Vulnerability**. Select the **Unique Vulnerability Count** checkbox.

Example:

Number of vulnerabilities when the Unique Vulnerability Count check box is not selected:



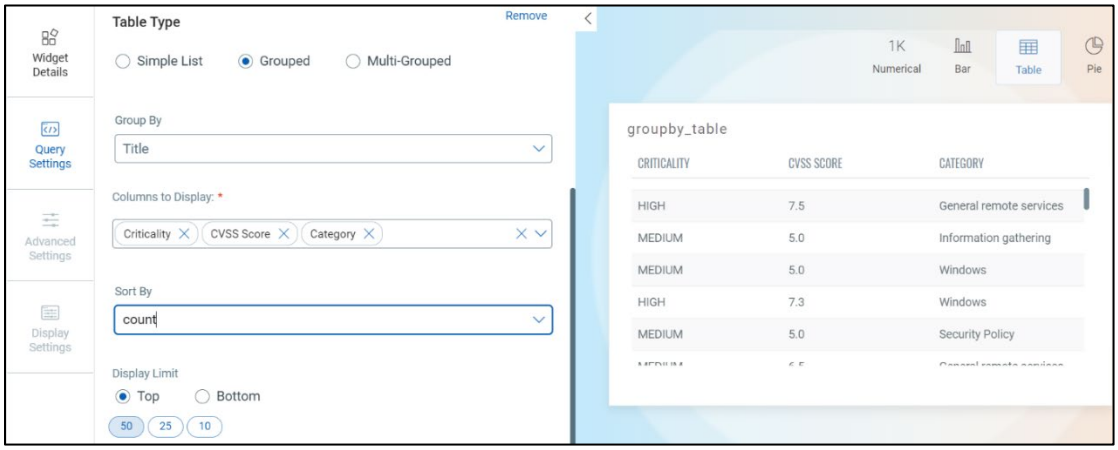
Number of vulnerabilities when the Unique Vulnerability Count check box is selected:



Columns to Display option for the Title Group By

The newly added option **Columns to Display** is added in the **Table > Group By** > **Title.** The **Columns to Display** option allows you to display additional columns in the Grouped Table Type.

Following are the supported fields that can be added in the Columns to Display: Count, Criticality, Title, CVSS Score, CVE IDs, Severity, Operating System, Qualys Patchable, Patch Available, Published Date, Updated Date, Category, and QID.



New Tokens Support

We have updated the information for the Vulnerability and Asset tokens to enhance your search results:

- **vulnerabilities.vulnerability.criticality:** Added support for the CVSS score that defines the criticality.
- **lastLocation.name:** Search the assets based on the last location.
- **lastLocation.continent:** Search the assets based on the continent of the last location.
- **lastLocation.country:** Search the assets based on the country of the last location.
- **lastLocation.state:** Search the assets based on the state of the last location.
- **lastLocation.city:** Search the assets based on the city of the last location.
- **lastLocation.postal:** Search the assets based on the postal of the last location.

Issues Addressed

AM AssetView

- We have fixed an issue, where the EC2 connector fetched the Virtual Private Cloud (VPC) with two regions.

TP Threat Protection

- We have fixed an issue, where the users could not assign tags and access the previously created dashboards.

CA Cloud Agent

- We have fixed an issue where the 'Last Activity' and 'Last Checked In' column names in the CSV report were swapped as compared to the sequence of columns in the user interface and incorrect values were getting displayed in these columns.
- We have added a note in the Activate Agent screen for VM, PC and SCA to inform users that the module will not be activated for the agent if the respective toggle key is set to OFF.

WAS Web Application Scanning

- We have fixed an issue, where WAS displayed an error message "An error occurred while processing web application. Please contact your account manager Invalid DOMAIN format" for domains or subdomains value while creating a web application.