Qualys Cloud Platform v3.x

Release Notes

Version 3.4
December 23, 2020

Here's what's new in Qualys Cloud Suite 3.4!

AV AssetView

TP ThreatProtect

New RTIs and Tokens Introduced: Ransomware, Solorigate/Sunburst

VMDR Vulnerability Management Detection and Response

New RTI Introduced: Ransomeware
Prioritization Report With More Patch Details
Enhanced Column Widget
New Fields Added to "Group By" Search Results for Vulnerabilities
New Fields Added to "Group By" in Widget Builder
New Tokens Updates
Additional OS Information

UD Unified Dashboard

New Templates for Dashboards

Administration Module

Exclude Cloud Agent Assets Added for IP Range Tags

Qualys Cloud Platform 3.4 brings you many more Improvements and updates! Learn more

AV AssetView

TP ThreatProtect

New RTI and Token Introduced: Ransomware

We now added support for Ransomeware and Solorigate Sunburst Real-Time Threat Indicator (RTI) for you to help you quickly search for assets that could be vulnerable to these threats.

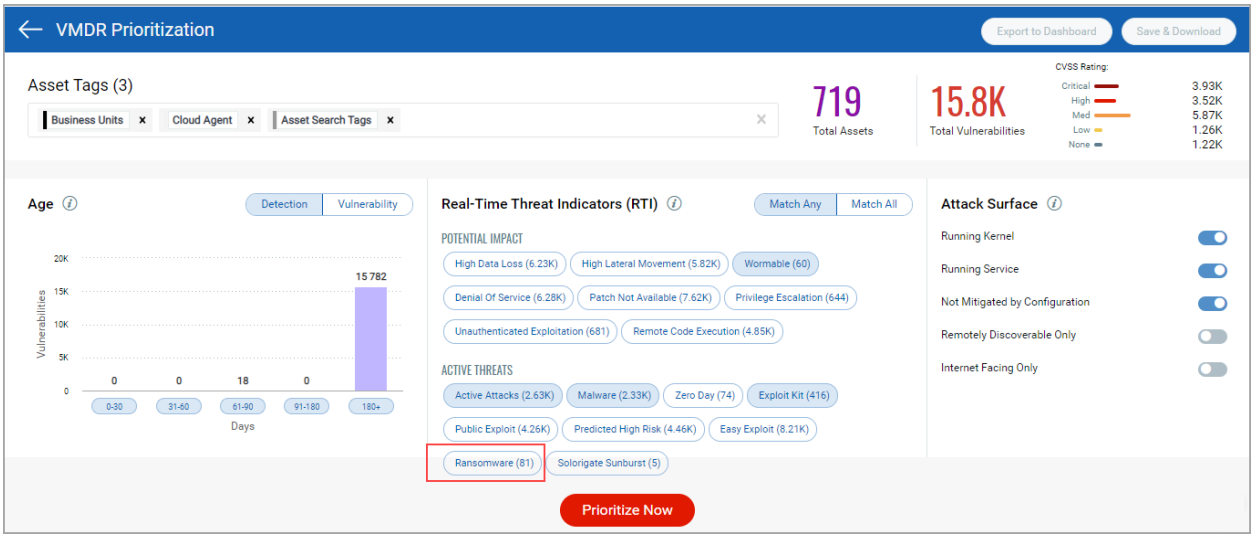
We have introduced the search tokens to enhance your search results for vulnerabilities associated with the new RTIs that we have introduced.
- `vulnerabilities.vulnerability.threatIntel.ransomware`
- `vulnerabilities.vulnerability.threatIntel.solorigateSunburst`

VMDR **Vulnerability Management Detection and Response**

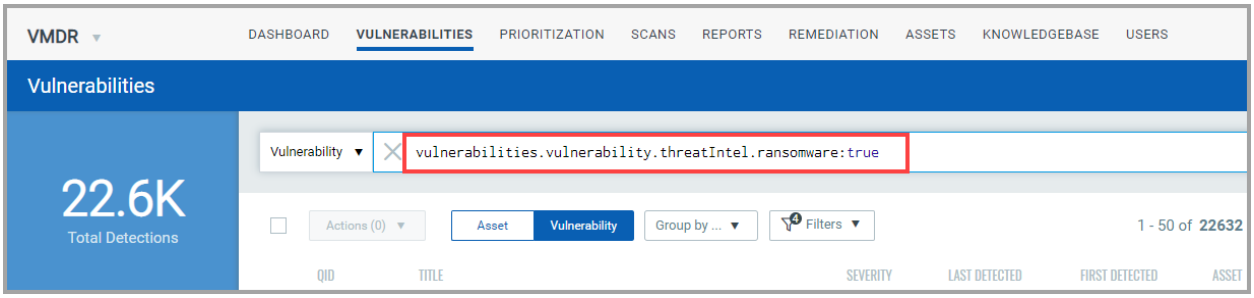
New RTI Introduced: Ransomeware

We have now introduced new Real-Time Threat Indicator (RTI) for you to help you quickly prioritize assets that could be vulnerable to Ransomware threat.

When you generate prioritizaion report, in the RTI section, you can notice the new RTI available for selection.

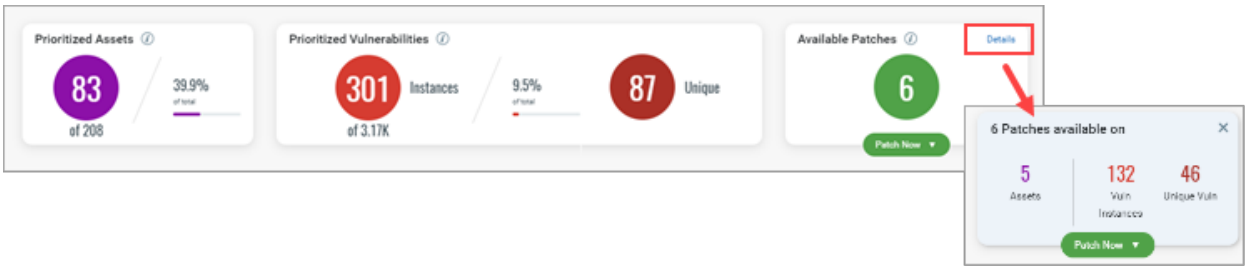


Use our new search token `vulnerabilities.vulnerability.threatIntel.ransomware` to simplify your search for assets exposed to ransomeware vulnerability.



Prioritization Report With More Patch Details

We now provide you with more information related to available patches in the Prioritization report. Details such as number of vulnerabilities that will be fixed with the available patches, - number of assets on which the vulnerabilities is detected and can be fixed with the patches.



In Available Patches section, click the Details link to view additional details that we provide.
Assets: The count of assets on which the vulnerabilities can be fixed with the available patches.
Vuln Instances: The count is the total number of vulnerabilities that meet the combination of the detection age, RTIs, and attack surface you selected that can be fixed with the available patches.
Unique Vuln: The count of unique vulnerabilities (excluding duplicate QID instances) that can be fixed with the available patches.

You could click on the Assets or Unique Vuln count to filter the data and view the asset/vulnerability details in the Details section.

Enhanced Column Widget

We have now enhanced our widget builder to create grouped or multi-grouped column widget. You can now consolidate various data points and group them using a single or multiple parameter in grouped or multi-column widget. We have now added two new column widget representation to simplify representation of multiple data points. The two new column widget types are Grouped and Multi-Grouped.

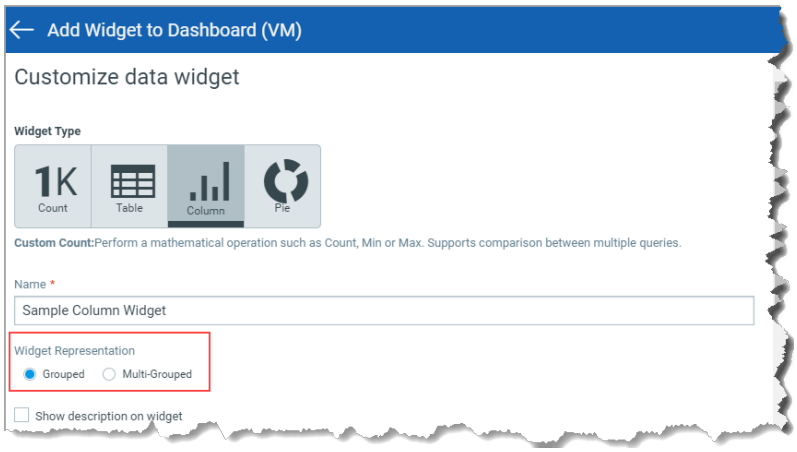
Note: The enhanced table widget types are available only for Vulnerability Management app.

On the dashboard, click the **Add Widget** button. In the widget builder, select **Vulnerability Management** application from the left pane and click **Create Widget**.

Choose the **Column** Widget Type.

You can view the new options in Widget Representation field.

Select the required type of representation.

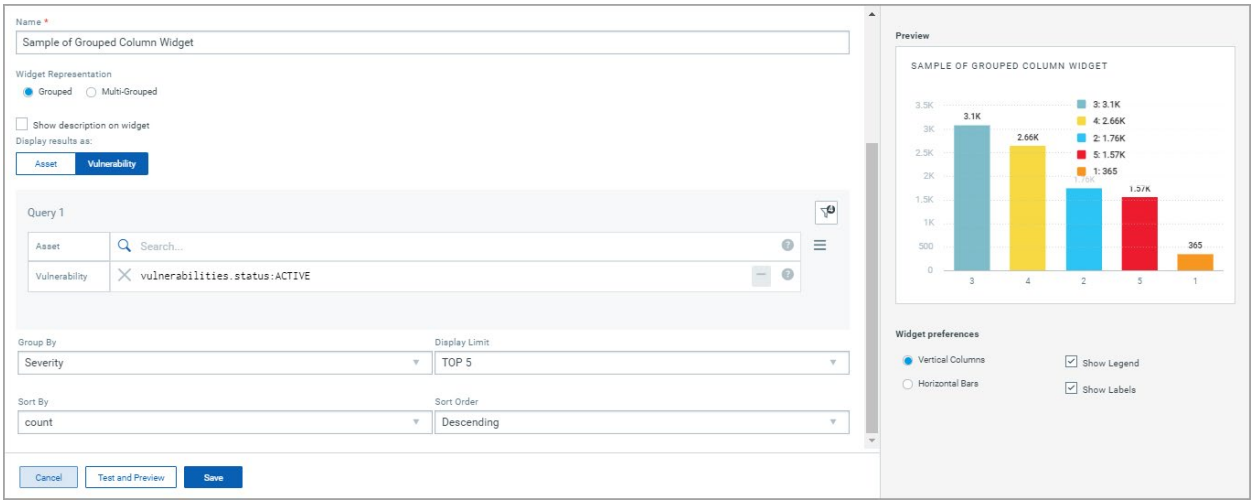


You can view the preview of the widget and configure the parameters as per your requirement. Click **Add to Dashboard** to complete widget creation and view the widget on the dashboard.

Grouped Column Widget

You can consolidate data points and group them using a single parameter in grouped column widget.

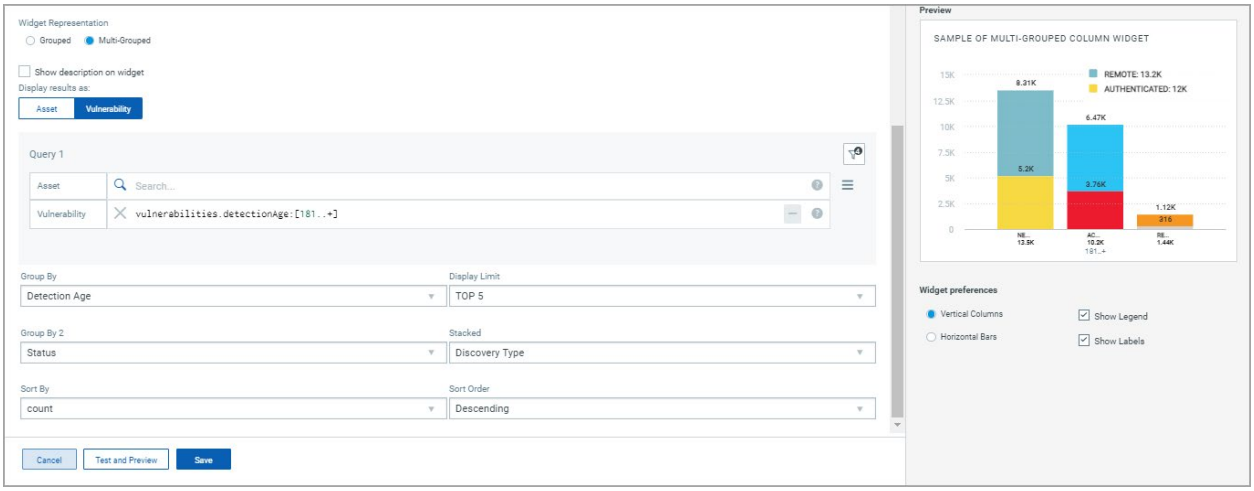
For example, you can view top 5 ACTIVE vulnerabilities (status as ACTIVE) that are grouped by severity and sorted in descending order.



Multi-Grouped Column Widget

You can consolidate various data points and group them using multiple parameters in multi-grouped column widget.

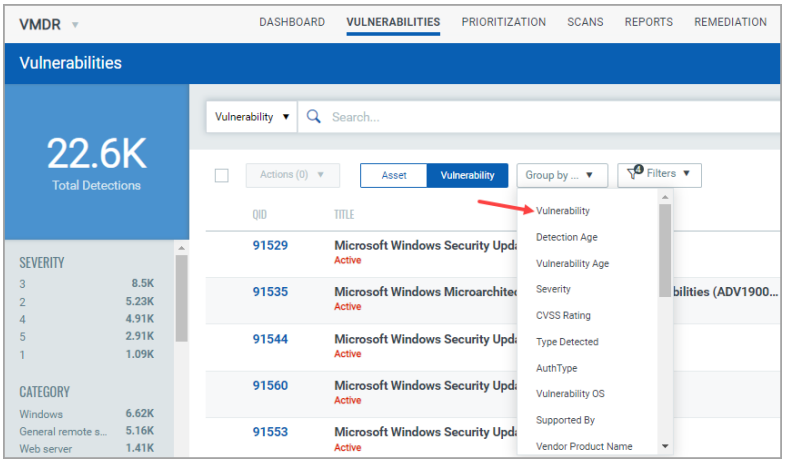
For example, you can view top 5 vulnerabilities of detection age with its multiple parameters such as status and discovery type sorted in descending order.



New Fields Added to “Group By” Search Results for Vulnerabilities

We have now made following additions to “Group by” to simplify your seach results for vulnerabilities.

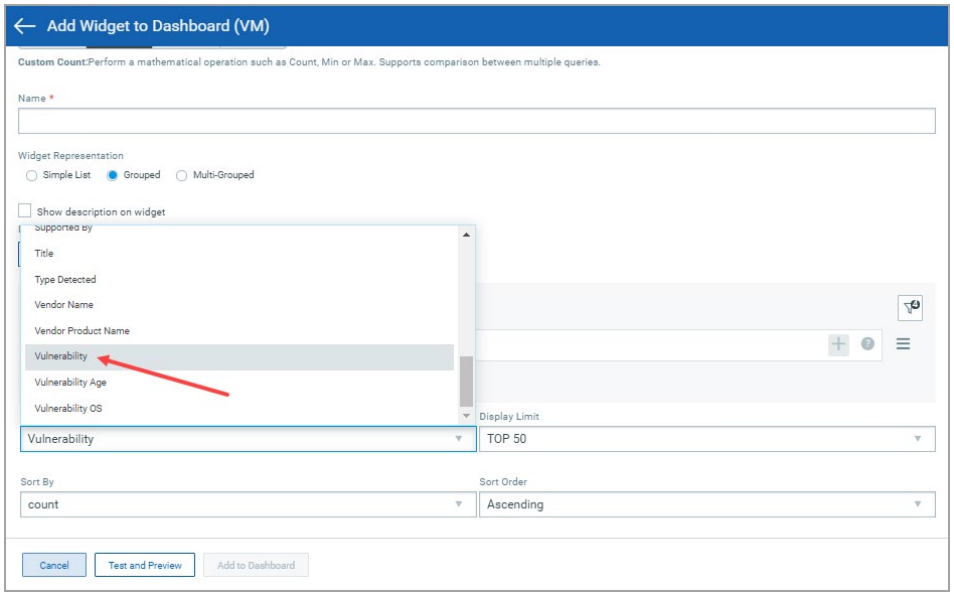
- Vulnerability (by QID)
- Category
- Port
- Reboot Required



New Fields Added to “Group By” in Widget Builder

We have now added “Group by” support for following fields/search tokens in the widget builder:

- Vulnerability (by QID)
- Category
- Port
- Reboot Required
- Compliance Type
- DiscoveryType/trackingMethod
- CVSS Score
- Published

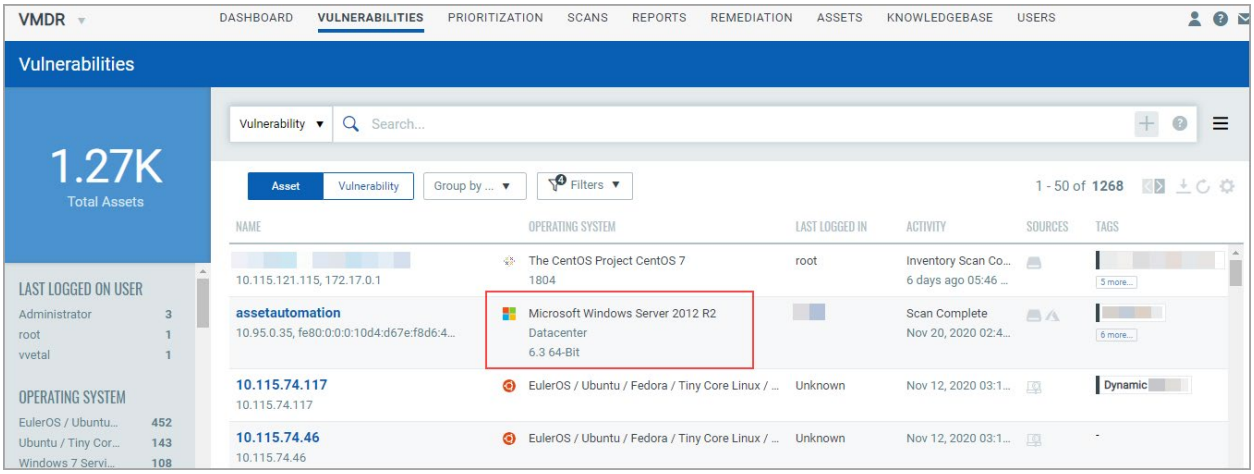


New Tokens Updates

We have introduced two new search tokens to enhance your search results:
- vulnerabilities.vulnerability.threatIntel.ransomware
- vulnerabilities.ssl
- vulnerabilities.vulnerability.rebootRequired

Additional OS Information

We now provide you additional information regarding the operating system of an asset. For example, you may view additional details related to the operating system such as bit related information, version details and so on.



Note: You need to have Global Asset Inventory app enabled for that asset in your subscription.

UD **Unified Dashboard**

New Templates for Dashboards

We have now enhanced our template library with addition of three new templates. You can use these pre-defined template dashboard to have a single-pane-of-glass view on the dashboard for assets with specific areas of concern.

The new templates that we have introduced in this release are:

- **Qualys Severity 1 - 5 & Threat Protection** – Provides Qualys Severity Scale and the Threat Protection RTIs with severity 1 to 5 as well as "Easy exploitable & Patchable".
- **Top 10 Vulnerabilities Scorecard** – Provides top 10 vulnerabilities in various states such as New, Active, Reopened, Ignored and Fixed.
- **Buffer Overflow & Kernel Vulns** – Provides high-risk vulnerabilities in GRand Unified Bootloader version 2.

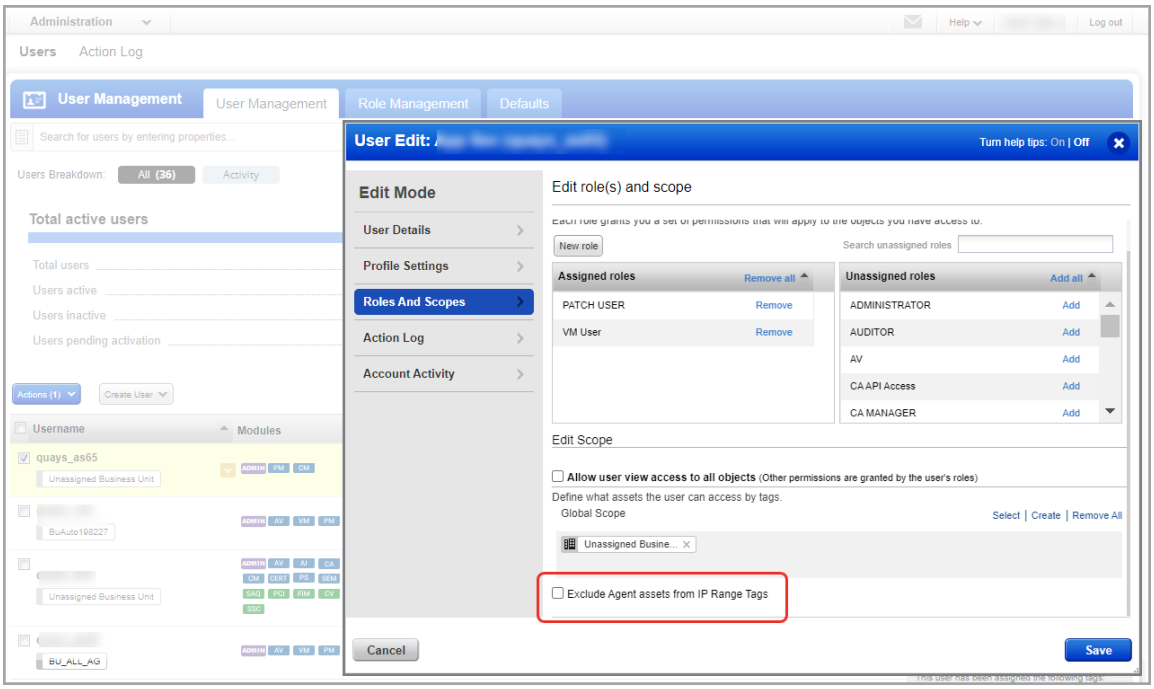
Administration

Exclude Cloud Agent Assets Added for IP Range Tags

We now give an option to exclude the Cloud Agent assets that are added to a sub-user scope due to the IP range tags in the Asset View module.

To exclude the Cloud Agent assets, the Manager user can select the required sub-user from the Administration module and click **Edit**. On the User Edit screen, select **Roles and Scopes** > **Exclude Agent assets from IP Range Tags** option.

Note: Cloud Agent assets added due to IP range tags cannot be excluded from Manager's asset scope.



Issues Addressed

We have fixed the following issues in this current release-

AV AssetView

- We have now fixed an issue where DNS name was displaying multiple times under DNS hostname on Asset View UI in the Asset Summary of an asset.
- The fix addresses an issue where creating AV connectors via API for 1 gov cloud region would set both regions in the connector and hence not honor the user provided input. The fix ensures that the regions on the connector will be set as per the user input. This affects only GovCloud connectors in AV.

CA Cloud Agent

- Fixed an issue where versions were only partially visible on Version Distribution widgets in Cloud Agent Dashboard.
- Fixed an issue where assets were wrongly tagged when an external IP address was used for tagging in the absence of IPv4 and IPv6 addresses.

WAS Web Application Scanning

- We fixed an issue where some of the scheduled scans were getting skipped due to a null web app ID in the previous scan which was stuck in the processing state. After the fix, the next scheduled scan is getting picked successfully by marking the previous stuck scan into the error state.
- We fixed an issue where an error message "An unexpected error occurred during report creation" was displayed when the user tried to open/download scan reports for old scans. After the fix, you can now download the scan reports in all formats for old scans.
- We will now show the latest non-retest scan information for the web application in the "last scan" field in the response when you make a call to the Get Web Application Details API.
- We fixed an issue where during a retest for a WAS Detection, the "Last Time Detected" field was getting updated even though findings in the detection could not be tested. After the fix, the "Last Time Detected" field in the detection gets updated only when Finding is detected.
- We fixed an issue where the user even though has required permission was getting an "Unauthorized" response when using the Get DNS Override Details API to get the DNS override information. After the fix, the user was able to get the DNS override information using the Get DNS Override Details API.

Administration

- We have now fixed an issue so that the action log for users in the Administration module is sorted in the correct order.

Qualys Cloud Platform

- Purging data of duplicate of a widget resulted in the loss of trending data for the widget. We have now fixed the issue so that purging the data for duplicate of a widget, results in loss of data only for the duplicate widget.