



Qualys Cloud Platform v3.x

Release Notes

Version 3.13

September 22, 2022

Here's what's new in Qualys Cloud Suite 3.13!

VMDR Vulnerability Management, Detection, and Response

[Vulnerability Details in Detection Summary of Vulnerability Tab](#)

[Detections by Status Shows the List of Vulnerabilities](#)

[New CISO Focused Dashboard Template](#)

CM Continuous Monitoring

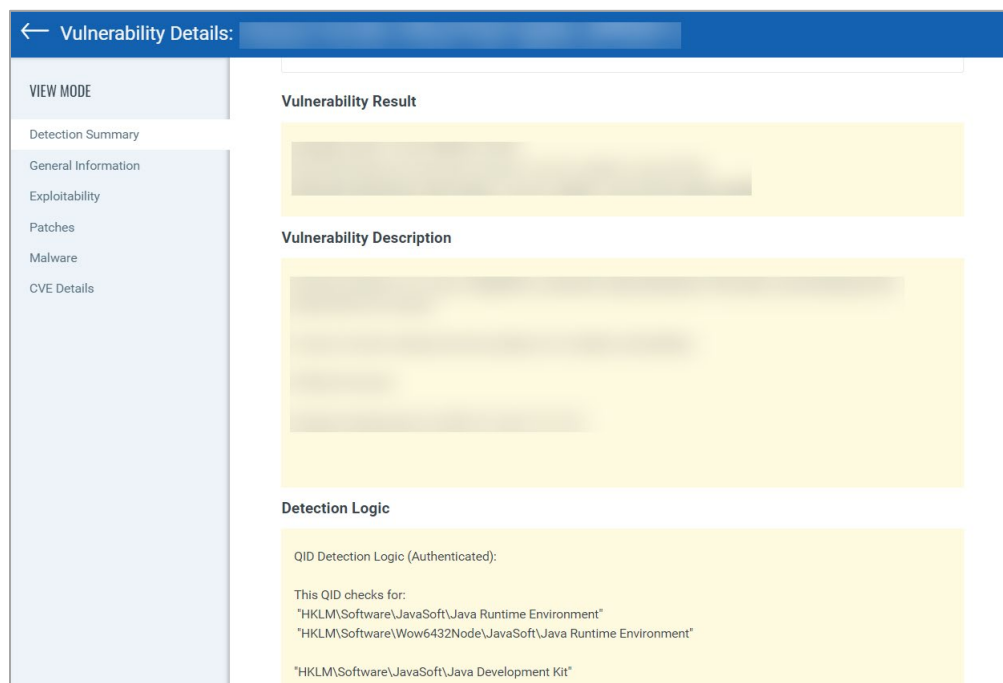
[Permissions Updated for Reader, Unit Manager, and Remediation User Roles](#)

Qualys Cloud Platform 3.13 brings you many more improvements and updates! [Learn more](#)



Vulnerability Details in Detection Summary of Vulnerability Tab

With this release, we have added the Detection Logic section. This feature makes it feasible for a user to go through the vulnerability information and detection logic at a glance. If a QID does not have a detection logic, the Detection Logic displays N/A.



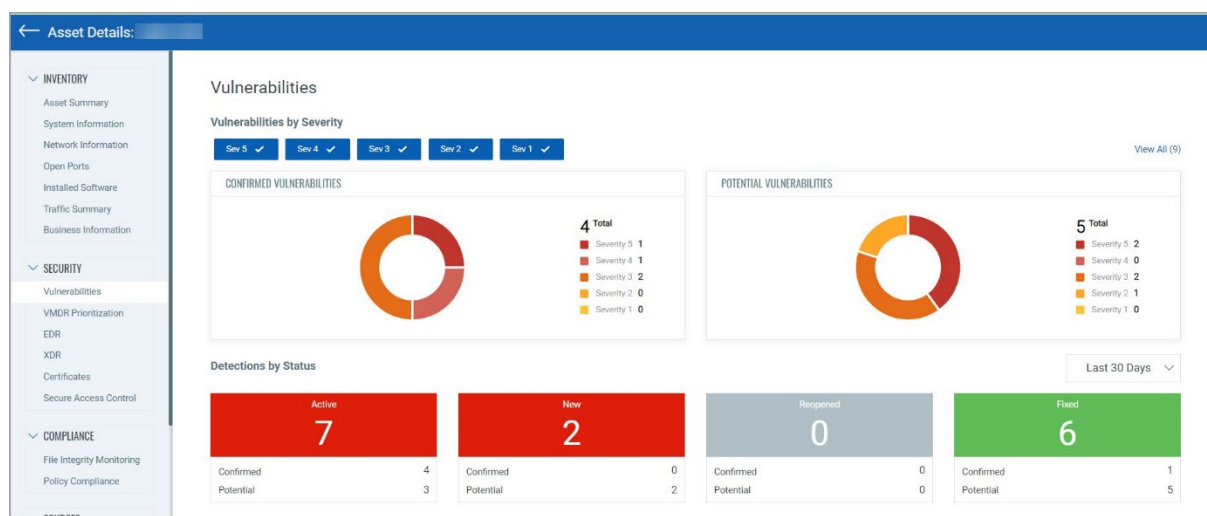
Detections by Status Shows the List of Vulnerabilities

With this release, we have introduced the clickable event in the Detections by Status section. This improvement gives you a summarized list of vulnerabilities on the asset. The Detection by Status is based on the Date selection and Vulnerability by Severity. If an asset does not have data within the selected time, the scores in the Detection by Status appears as 0.

The following steps are a walkthrough about the clickable event for Detections by Status

1. In the **Vulnerabilities** tab, select **Asset**. Select an asset to view its details.
2. In the **Security** section, click **Vulnerabilities**.
3. Select the severity in **Vulnerabilities by Severity** for the asset, **Detections by Status** displays the score of **Active**, **New**, **Reopened**, or **Fixed**.
4. Click on the total score displayed in **Active**, **New**, **Reopened**, or **Fixed**.


For example, in the following screenshot, the **Fixed** status displays the total score as 6. Click the score, and you are redirected to the fixed Vulnerabilities list.

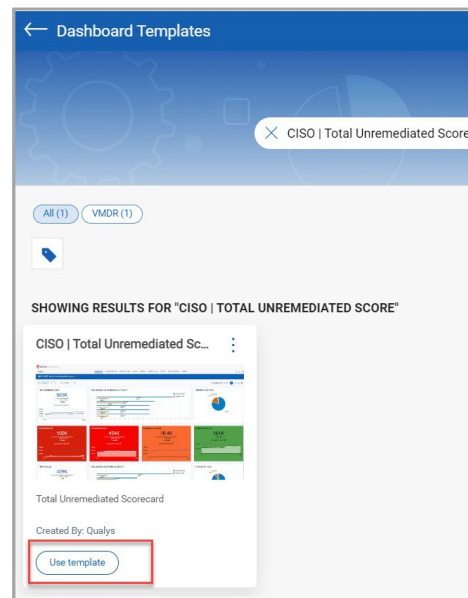


New CISO Focused Dashboard Template

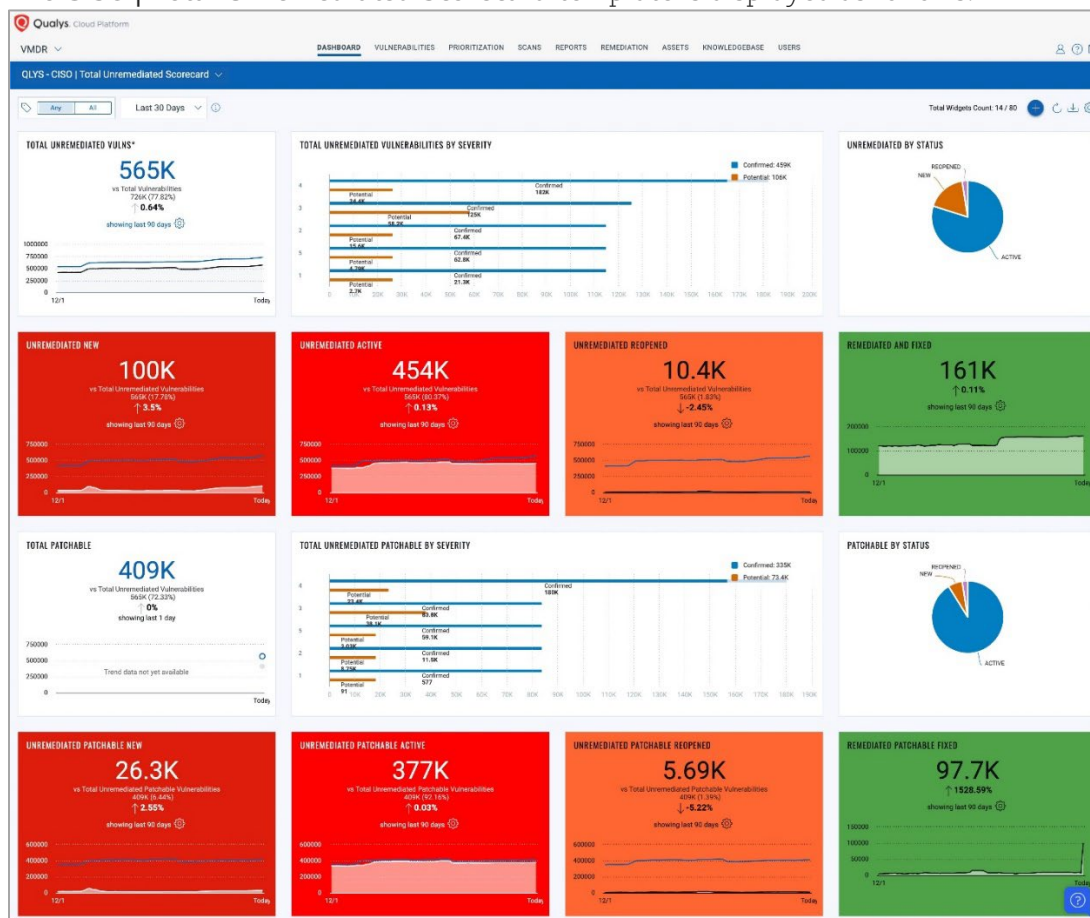
With this release, we have introduced **CISO | Total Unremediated Scorecard** template for the VMDR application. Using the **CISO | Total Unremediated Scorecard** dashboard template, you can track the unremediated vulnerabilities using **Group by** - Severity or Status. The template also provides the number of vulnerabilities that have a patch available and the score of fixed vulnerabilities after applying the patch.

Perform the following steps to use the template:

1. In the **VMDR** application, click .
2. Select **Create New Dashboard**.
3. In the **Search for Dashboard Templates** search bar, type **CISO | Total Unremediated Scorecard**.
4. Click **Use Template**.



The **CISO | Total Unremediated Scorecard** template is displayed as follows:



Permissions Updated for Reader, Unit Manager, and Remediation User Roles

With this release, we have updated the user role permissions for the reader, unit manager, and remediation in the Continuous Monitoring application. This update allows you to customize the permission options in the Continuous Monitoring application. The user role permissions are updated for:

- View Monitoring Profiles
- View RuleSets
- View, Hide, and Flag Alerts

The screenshot shows the 'Role Edit: CMRULEREADER' interface. On the left is a sidebar with 'Edit Mode' containing 'Role Details', 'Permissions' (selected), and 'Action Log'. The main area is titled 'Edit permissions for this role' and includes a 'Modules' search bar. Below, 'Role Permissions by Modules (13)' lists the 'CM' module. A red box highlights the 'CM Permissions (13 of 13)' section, which contains a list of permissions, all of which are checked: 'CM UI Access', 'Create Monitoring Profile', 'Edit Monitoring Profile', 'View Monitoring Profile', 'Delete Monitoring Profile', 'Enable/Disable Monitoring Profile', 'Create Ruleset', and 'Edit Ruleset'. At the bottom are 'Cancel' and 'Save' buttons.

Module	Permission	Status
CM	CM UI Access	<input checked="" type="checkbox"/>
	Create Monitoring Profile	<input checked="" type="checkbox"/>
	Edit Monitoring Profile	<input checked="" type="checkbox"/>
	View Monitoring Profile	<input checked="" type="checkbox"/>
	Delete Monitoring Profile	<input checked="" type="checkbox"/>
	Enable/Disable Monitoring Profile	<input checked="" type="checkbox"/>
	Create Ruleset	<input checked="" type="checkbox"/>
	Edit Ruleset	<input checked="" type="checkbox"/>

Issues Addressed

VM

Vulnerability Management

- We have fixed an issue where users were unable to sort vulnerability data using the Severity option in the Sort By field after selecting Severity in Group By field.
- We have fixed an issue where additional queries were added in the QQL when users selected table type as Mutil-Grouped for Table widget. The additional queries do not get added to the QQLs.
- With this release, we have fixed an issue where users can retrieve service name information for agent-tracked assets. Following are the impacted APIs:
GET: <API server name>/qps/rest/2.0/get/am/hostasset/{assetid}
SEARCH: <API server name>/qps/rest/2.0/search/am/hostasset/{assetid}
- We have fixed an issue where the published date in the VMDR CSV report was incorrect. The VMDR CSV report now includes the correct published date.
- We have fixed an issue where the Qualys Detection Score (QDS) pop-up did not show the correct QID number if a CVE was not associated with the QID.
- We have fixed an issue where incorrect asset count was shown for widgets and asset search if the search criteria used a vulnerability QQL with the NOT operator.
- Previously, when a user exported the dashboard from the Asset View application to Unified Dashboard, the query would populate in the Vulnerability Query field of the Unified Dashboard widget. With this release, we have fixed an issue where when a user exports a new dashboard from the Asset View application to Unified Dashboard, the action populates the query in the Asset Query field of the Unified Dashboard. From this release, all the newly created Asset View application queries, including the vulnerabilities token, if exported to Unified Dashboard, will be considered an asset query in the Unified Dashboard.
- We have fixed an issue where connectors were not found when the user tried to launch Azure Cloud Perimeter Scan. The API now fetches only the required fields reducing the unrequired database call.
- With this release, we have fixed an issue where Qualys agents were uninstalled due to falsely marking of the assets as deleted.

WAS

Web Application Scanning

- We have fixed an issue where the subusers could not delete the scan schedules that they had created.
- We have fixed an issue where the user could not download the web application and scan reports from WASUI when the user edits the report or uses a template with a dynamic search list that includes confirmed and potential severity.

CA

Cloud Agent

- We have fixed an issue where the agent list report downloaded from Cloud Agent UI did not contain any data.