Qualys Cloud Platform v2.x

Release Notes

Version 2.42.2
December 16, 2019

Here's what's new in Qualys Cloud Suite 2.42.2!

MD **Malware Detection**

WAS **Web Application Scanning**

New Actions for Vulnerabilities in Knowledgebase

Qualys Cloud Platform 2.42.2 brings you many more Improvements and updates! Learn more

MD **Malware Detection**

WAS **Web Application Scanning**

New Actions for Vulnerabilities in Knowledgebase

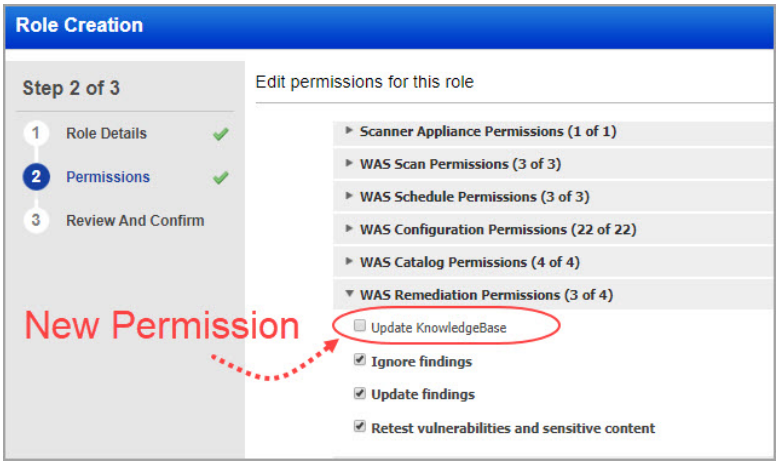
We have now introduced new actions for vulnerabilities in your knowledgebase. You can now:
- edit the severity of a vulnerability
- restore severity of a vulnerability
- ignore a vulnerability
- activate a vulnerability

The actions are applicable for QIDs in KnowledgeBase for both modules: Web Application Scanning and Malware Detection.

Note: This feature is not available by default. Contact Qualys Support to get this feature enabled.

What Permissions are Needed?

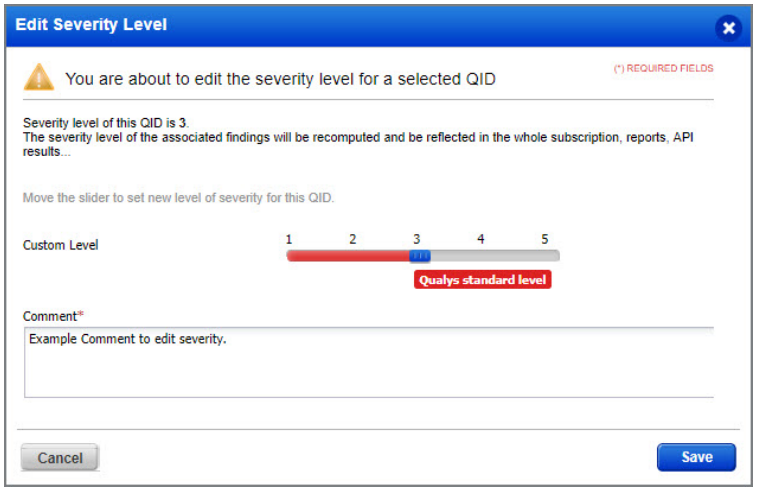
We have introduced a new permission named "Update Knowledgebase" in WAS Remediation Permissions (Malware Remediation Permissions in MDS) for a user to be able to perform the new actions that are introduced for vulnerabilities.



By default, this permission is assigned only to Manager user. If you want other users to be able to perform the actions, you need to explicitly assign Update Knowledgebase permission to the user.

Edit Severity

Go to Knowledgebase, select the QID of the vulnerability and then select Edit Severity from the Actions menu.



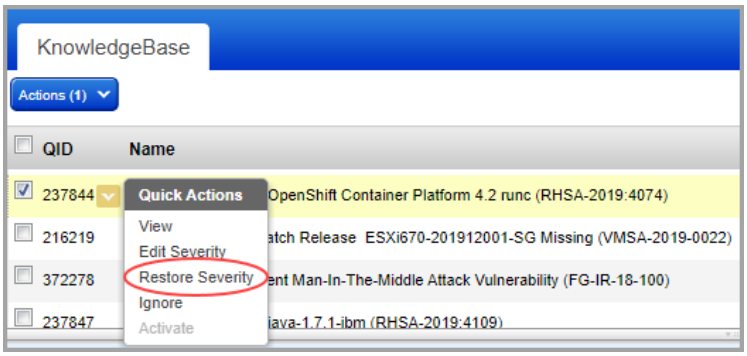
Slide the slider for Custom Level to the level you want to assign to the selected QID.

Add a comment to indicate the change or reason for the change and then click Save.

Restoring Severity

If you have changed the severity of a QID and want to revert it to the Qualys defined severity, select the QID, and select Restore Severity from the Actions menu.

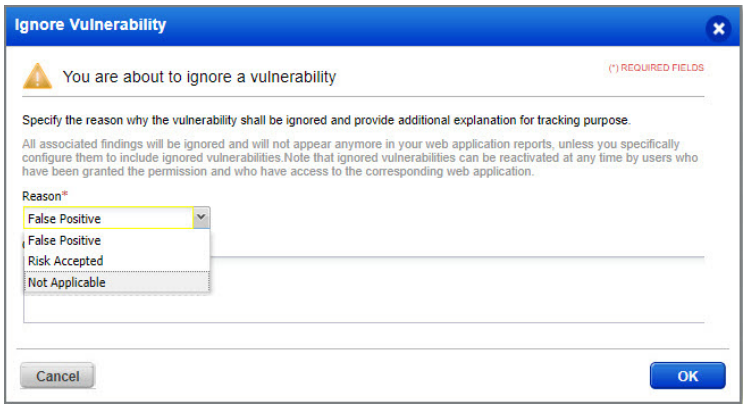
A message is displayed asking confirmation for restoring severity of the QID. Once you confirm, the severity of the QID is restored to the Qualys defined severity.



Ignoring a vulnerability

You can ignore vulnerabilities so they don't appear as actionable issues in the detections list.

Go to Knowledgebase, select the QID and select Ignore from the Actions menu. When you ignore a detection, you'll be prompted to give a reason - false positive, acceptable risk or not applicable. The ignored detection's status label is grayed out in the report and in the Detections list.

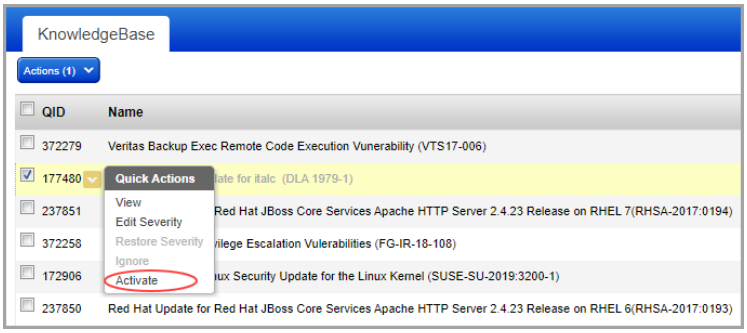


By default, the detection will not appear in future reports on the same web application or scan (or site for MDS), until it is reactivated.

Activating a QID

If you have marked the vulnerability as Ignore and now want to activate the vulnerability, select the QID, and select Activate from the quick actions menu.

A message is displayed asking confirmation for activating the QID. Once you confirm, the QID is not ignored.



Issues addressed in this release

Qualys Cloud Platform 2.42.2 brings you many more improvements and updates.

AV AssetView

- Fixed an issue where the AssetView module failed to launch in Internet Explorer.

CA Cloud Agent

- Fixed an issue where the simultaneous assignment of configuration to a large number of agents was taking longer than expected.

WAS Web Application Scanning

- We have now significantly improved on the time needed to load the complete detection list. However, the Preview tab in the detection list may take some extra time to display data.
- We have now added validations for POSTMAN file upload so that users can successfully upload supported files and appropriate message is displayed for incorrect files. Users can now upload POSTMAN collection file based only on the below validations:

  - Presence of '_postman_id' field in the info node

  - Domain name of the schema field value should match schema.getpostman.com

  - In the schema field, the version number v2.0.1 or v2.0.0 are valid/supported versions