Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.23.1

August 25, 2023

This new release of the Qualys Cloud Platform (VM, PC) includes improvements to Vulnerability Management and Policy Compliance.

Qualys Vulnerability Management (VM)

First-Party Risk Management: Custom Vulnerabilities (QIDs)

Qualys Policy Compliance (PC/SCAP/SCA)

Support for New Authentication Technologies

Qualys 10.23.1 brings you many more improvements and updates! Learn more

What's New?

First-Party Risk Management: Custom Vulnerabilities (QIDs)

Organizations use first-party software that is software developed in-house and used to run businesses. Security teams face a major challenge in securing first-party applications due to the constantly changing attack surface.

With this release, you can now identify potential risks in first-party and open-source software. You can now define custom vulnerabilities by creating your own detection and remediation scripts in Qualys VMDR and get a comprehensive overview of all vulnerabilities in your environment. The scripts can be created using commonly used languages such as PowerShell and Python in VMDR. Vulnerabilities are detected based on the logic defined in scripts.

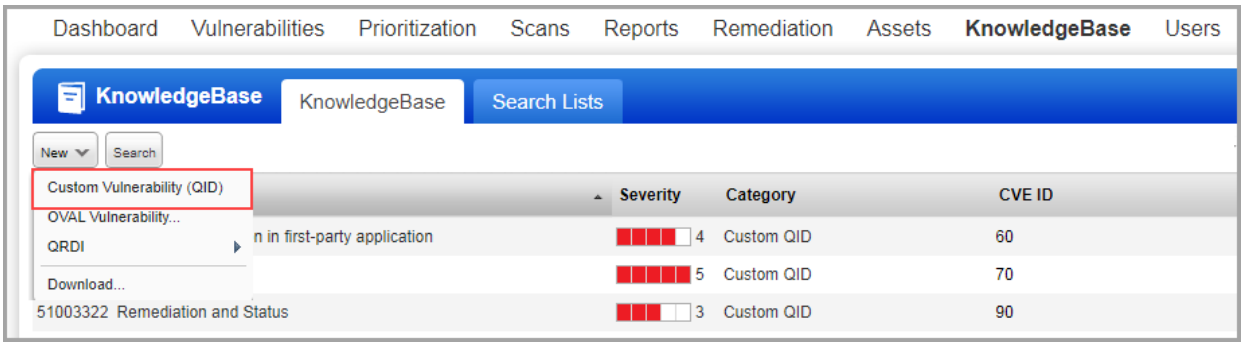
When defining a custom vulnerability, you need to specify various parameters such as vulnerability type, severity level, and QID type. These vulnerabilities are stored in the KnowledgeBase with their QIDs. You can view their category as **Custom QID** and use them in the same way as standard vulnerabilities for detection.

To know more about this feature, refer to Online Help: Creating Custom QIDs and Searching for Custom QIDs.

Prerequisites

- To use this feature, the account must be Vulnerability Management Scan Processing (VMSP) enabled. Contact Qualys support for more information.
- To support this feature, you must have Qualys CAR application with version 1.8.0.0 or later.

Furthermore, custom QIDs are available as part of the Host List Detection API. For more information on API, refer to the Qualys VM-PC API Guide.



Support for New Authentication Technologies

With this release, the following technologies are now for Policy Compliance authenticated scans using scanners:

- IBM DB2 z/OS 13.x
- VMware vCenter Server Appliance 8.x
- VMware ESXi 8.x

For more information, see Authentication Technologies Matrix.

Issues Addressed

The following issues are fixed with this release:

- While adding hosts to a scan using asset tags, the **Add Tags to Include** dialog box displayed a **"Show more"** link at the end of the list. However, upon clicking the link, no additional tags were shown. This issue is now fixed.
- We have fixed an issue in the **Scans** tab (VM) where irrelevant search results were fetched when using a two-character search string.
- We have fixed an issue related to the report template generated using the report creation API. Previously, if the template did not include the Threat, Impact, and Solution columns, they would still be added to the report.
- We have fixed an issue where the end users got an error message in the API response if more than 910 QIDs passed in the API call request. The issue was fixed by providing an API call using POST along with the existing GET method.
- We have addressed the query about the functioning of the scanner appliance heartbeat check notification by adding a detailed explanation to understand how it works. For more information, refer to Online Help: Scanner Appliance Heartbeat Check Notification.
- We have fixed an issue where & was getting shown as &amp in the scan list API call.
- We have fixed an issue where the compliance report was not showing data for all assets for sub-users when **Asset Tag Scoping** was enabled, and the report launched on the asset tags.
- We have fixed an issue where the Ignore Vuln API was failing due to an internal error (999).
- We have fixed an issue with the Host List Detection API response, where the EC2 metadata attribute, Instance Type, was missing. To fix this, we recommend adding instance-type to the host_metadata_fields.
- We have fixed the issue of stack trace leaks, which caused critical data to be printed in log files whenever an exception occurred.
- We have fixed an issue where custom control CID 100044 failed on the host, even when both OS and DB level authentication were successful.
- We have fixed an issue where the Host List Detection API response included assets associated with asset tags that were excluded in the request call.
- We have fixed an issue where the Host List Detection API response contained the QID results section despite the 'show_result' parameter being set to zero in the request call.
- We have fixed an issue where the option profile dropdown was not sorted alphabetically.
- We have fixed an issue where the Host List Detection API, Scheduled Report, Asset Host List API, and EC2 scheduled scan were unable to fetch data.