Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.25.2

January 22, 2024

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

What's New?

Qualys Vulnerability Management (VM)

Auto-enabling of DNS Tracking Setup for Hosts

Qualys 10.25.2 brings you many more improvements and updates! Learn more

Auto-enabling of DNS Tracking Setup for Hosts

With this release, Qualys has auto-enabled DNS tracking Setup which helps in monitoring the communication between the client and the server. Earlier, users with **Scan by Hostname** service subscriptions had to send a request to Qualys to enable the **DNS Tracking Setup**. This enhancement automatically sets the tracking method to DNS for hosts when a valid DNS hostname is detected. This helps to reduce the time to enable the **DNS Tracking Setup**, and users quickly benefit from this setup.

Issues Addressed

The following issues are fixed with this release.

Component/Category	Application	Description
PC - UI	Policy Compliance	The **Account Info** (Go to **Help** > **Account Info**) displayed an incorrect number of unique hosts that have been scanned. The relevant code changes have been made to fix this issue.
PC - UI	Policy Compliance	The user encountered an error while creating a new Widows User Defined Control with Data Type: Integer and Operator other than IN. The relevant code changes have been made to fix this issue.
PC - UI	Policy Compliance	When the PC/SCA application expired, the user was still able to see Ips and able to filter it in the **Address Management** tab. Now, the filtering option will no longer be available for expired subscriptions. As a result, the user will not be able to view the IPs of the expired subscriptions on the **Address Management** tab.
PC - Scan Backend	Policy Compliance	The users with both PC and SCA cloud agents experienced a significant delay during PC scan execution. The relevant code changes have been made to fix this issue.
PC - API	Policy Compliance	On executing the Scheduled Reports List API, the API response did not include the SCA scheduled reports list. The relevant code changes have been made to fix this issue.
PC - API	Policy Compliance	On executing the PC Posture Information API with the Host ID (Ips) parameter, the API returned an incorrect response. The API response included the IPs removed from a tag that is associated with a policy. The relevant code changes have been made to fix this issue.
PC - New UI	Policy Compliance	The corresponding host records were not being updated after purging the asset/agent. This resulted in stale asset data being displayed in the Policy Compliance Posture. The relevant code has

		been modified to fix this issue.
VM - UI General	Vulnerability Management	The asset group details were not visible on the UI in the **Targets** column on the Schedule scan list page (Go to **Scans** > **Schedules**). The **Target** column was getting displayed blank. The relevant code changes have been made to fix this issue.
VM - Knowledge Base	Vulnerability Management	The Vulnerability Information for QIDs did not display complete Detection Logic (Unauthenticated and Authenticated). The relevant code changes have been made to fix this issue.
VM - Host List API	Vulnerability Management	When the user executed Host List API, the API response did not contain the FIRST_FOUND_DATE field information for Cloud Agent-tracked assets. The relevant code changes have been made to fix this issue.