Qualys Cloud Platform (VM, PC) 10.x

Release Notes

Version 10.22.2

May 18, 2023

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

Qualys Policy Compliance (PC/SCAP/SCA)

Support UDCs for Scanner and Agent on Debian GNU/Linux 11.x and OEL 9.x

API Changes

Refer to Qualys Cloud Platform (VM, PC) API 10.22.2 Release Notes for the API changes in this release.

Qualys 10.22.2 brings you many more improvements and updates! Learn more

What's New?

Support UDCs for Scanner and Agent on Debian GNU/Linux 11.x and OEL 9.x

Starting this release, Debian GNU and Linux 11.x now support the following UDC types for Scanner and Agent:

Supported for Agent and Scanner	Supported Only for Agent
• File/Directory Existence • File/Directory Permission • File Content Check • File Integrity Check • Unix Directory Search Check • Directory Integrity Check	• File Content Check • Script Result Check

Issues Addressed

The following issues are fixed with this release:

- We have fixed an issue where an agent couldn't perform VM scans for large XML files during agent scan processing.
- We have fixed an issue where the user account was locked, and logs were not populated under activity logs.
- We have fixed an issue where users were unable to change the owner of a few asset groups that have multiple domains with similarities in names.
- We have fixed an issue where the discovery scan was resolving the vulnerabilities incorrectly. Despite fixing the QIDs which were part of the custom search list it fixed the other QIDs. Now this issue has been resolved.
- We have fixed an issue where the PC and VMDR reports were stuck for generating at 4% and were not generated successfully.
- We have fixed an issue where compliance Posture API resulted in ORA error (ORA-01555). This was due to scheduled report tasks being deleted, which in turn deleted the tagset_ids associated with them and removed them from the platform. The tagset_ids are no longer deleted from the platform.
- We have fixed an issue where assets from other networks were shown in the compliance report even though the user does not have access to those assets.
- We have fixed an issue where the QID was detected in the report for an asset even though the CVE ID associated with the QID was not added in the dynamic search list to include in the report template.
- The user was using the list VM scanned hosts API with the output format specified as CSV_NO_METADATA_MS_EXCEL. Output data in a cell was overflowed and flooded in the next cell of the CSV file instead of truncating the length. We have fixed this issue; the data in all cells are displaying correctly and following the MS Excel restriction.
- The scan report link provided in the report notification email was inaccessible for reader users who had not launched the scan, even though the scan was within their scope of permissions. An error message stating "You are not allowed to view this page." was displayed. This issue is now resolved.
- The Host Detection List API *(/api/2.0/fo/asset/host/vm/detection/?action=list)* encountered failure due to an ORA error. The issue is now fixed.
- The Policy Compliance data collected by the agent or scanner was not getting updated on the user interface because it had not been processed for a significant period of time. We have fixed this problem by addressing the issue of Posture/Exception data deletion, which occurred when controls were removed from the policy at the policy or technology level.
- The PC posture information API *(/api/2.0/fo/compliance/posture/info/)* did not retrieve evidence information for the database UDCs. This issue is now fixed.