Qualys Cloud Agent Windows 4.9

September 2022

We're excited to tell you about new features, improvements, platform coverage changes, and fixes in this Cloud Agent release. These updates are specific to the agent binary. Platform updates for new features and fixes of management, syncing, tagging, and reporting capabilities of Cloud Agents are documented in the Cloud Platform and Cloud Suite release notes.

New Features

- Patch Management:
  - Patch job deployment workflow is enhanced to post detailed statuses to the backend to get better visibility on the deployment job progress.
  - With the patch management configuration, you can set the Powershell execution policy to bypass the Powershell execution policy on an asset to execute actions defined in the patch job successfully.
    This prevents a scenario where script executions and actions in the patch jobs can fail due to the Powershell execution policy on an asset.
    Note: When you configure the Powershell execution policy to override the execution policy settings on an asset, it is applicable only for the specific session. There are no changes made in the system-defined policy.
- Endpoint Detection and Response:
  - Added asset quarantine feature that can restrict network communication with a specific host in case of any malicious event. You can quarantine an asset from the Endpoint Detection and Response application.
    When an asset is quarantined, the asset will be isolated from the network and communicates only with the Qualys Cloud Agent. However, you can configure the applications that the quarantined asset can access.
  - Added new DLLs for Antimalware Scan Interface (AMSI) and quarantine asset feature. The DLLs will be downloaded from the POD to the `C:\ProgramFiles\Qualys\QualysAgent\EDR` directory.

Enhancements

- Cloud Agent uses C:\ProgramData\Qualys\QualysTemp directory to download and execute scripts for Custom Assessment and Remediation (CAR) or Patch Management instead of Windows\Temp directory. This prevents the scripts from getting incorrectly flagged as malicious.

Behavior Changes

There are no behavior changes in this release.

Platform Coverage Support (Operating Systems)

- Added ARM support for Windows 11 through x64 emulation support.

Note: Only Scan based modules are currently supported.

Fixed Defects

The following reported and notable issues have been fixed in this release.

CRM-93595 CRM-88132 CRM-90141	Fixed issues for agent uninstallation with Force=true parameter.
CRM-92568	Fixed an internal bug leading to incorrect detection of QID 87387 Oracle WebLogic Server Remote Code Execution Vulnerability.
CRM-93214 CRM-95423	Fixed an internal bug related to collecting the Security Descriptor field value.
CRM-88046	Fixed an internal bug that led to incorrect detection of QID 87467 - Oracle WebLogic Server Multiple Vulnerabilities.
CRM-91682	Fixed an issue where the Cloud Agent could not proceed with scanning when it encountered a corrupt or invalid manifest. Now, the Agent skips the corrupt or invalid manifest and scans for the other applications.
CRM-83697	Fixed an issue that caused a delay in scanning directories. Now, the Cloud Agent is enhanced to perform faster directory scans.

Known Limitations and Workarounds

There are no reported and notable issues open in this release.