Container Security v1.x

Release Notes for Jenkins Plugin

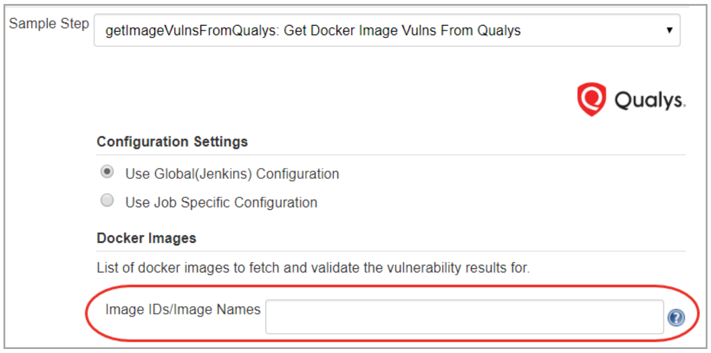
Version 1.5

March 28, 2019

Here's what's new in the Jenkins Plugin for Container Security!

Support for Docker Image Names

You can now provide names of the docker images you wish to scan for vulnerabilities. The plugin will try to fetch the corresponding image ID based on the provided image name.



Sample Step: getImageVulnsFromQualys: Get Docker Image Vulns From Qualys

Configuration Settings

● Use Global(Jenkins) Configuration

○ Use Job Specific Configuration

Docker Images

List of docker images to fetch and validate the vulnerability results for.

Image IDs/Image Names

While configuring a job specify an image name in the format repo:tag.

For more information see the "Define docker image Ids" section for "Qualys Vulnerability Analysis Plugin for Jenkins" in the Qualys Container Security User Guide.

Fixed issue

Fixed an issue where during job execution the test connection to Qualys Container Security API aborts after the first failed attempt (on receiving a 5xx family response from the server side. e.g., 500 Internal Server error). It will now retry every five seconds for three times.

Upgrade considerations

VERSION	DESCRIPTION
Upgrading from plugin version 1.4.2.0 to 1.5.0.0	Problem: Older reports not seen. Resolution: Re-run the build job.
	Problem: Job doesn't run if configured for "Exclude Conditions". Resolution: Re-configure the job with "Exclude Conditions", and then re-run the job.
Upgrading from plugin version 1.4.3.0 to 1.5.0.0	Existing reports are visible. Existing jobs run without errors.
Upgrading from plugin version 1.4.3.1 to 1.5.0.0	Existing reports are visible. Existing jobs run without errors.