Qualys Container Security

Release Notes for Sensor

Version 1.23
March 22, 2023

What's New?

Sensor Inactive Window for Registry Sensors
Connecting to JFrog Artifactory Private Registry with Non-Admin Credentials
SCA Scanning: Support for containerd Runtime
New Argument for Scanning Policy
Performing Only Static Scanning for Container Images

API Changes

Refer to the Container Security API 1.23 Release Notes for the API changes in this release.

Issues Addressed

Qualys Container Security Sensor 1.23 brings you many more improvements and updates! Learn more

What's New?

Sensor Inactive Window for Registry Sensors

You can now configure a sensor inactive window for registry sensors. Upgrade your registry sensor to version 1.23 or later to take advantage of this feature.

For more information about the sensor inactive window, see Online help: Managing Sensor Profiles.

Connecting to JFrog Artifactory Private Registry with Non-Admin Credentials

The registry sensor can now connect with JFrog Artifactory Private Registry with non-admin account credentials. As a result, when adding a JFrog Artifactory Private Registry for scanning, you can now authenticate using the credentials of a non-admin user. The non-admin user must have at least read access to the repositories under consideration.

This new feature allows you to scan your container images stored in JFrog Artifactory Private Registry with minimum privileges.

SCA Scanning: Support for containerd Runtime

The support for SCA scanning has been extended to the containerd runtime, making SCA scanning available to a broader range of environments. Previously, it was available only for the docker runtime.

For more information about SCA scanning, see Online help: SCA Scanning.

New Argument for Scanning Policy

While installing the sensor, you can now specify a new argument for the scanning policy, which allows you to select the suitable scan type as per your requirement. The new argument is not applicable to the CRI-O runtime.

The following table shows the usage of the new argument with possible values:

Sensor Deployment Method	New Argument	Available Values
installsensor.sh command (Binary installation)	Specify the argument in the installsensor.sh script: `ScanningPolicy=<value>`	• `DynamicScanningOnly`: performs only dynamic scanning. • `StaticScanningOnly`: performs only static scanning. • `DynamicWithStaticScanningAsFallback`: performs static scanning as a fallback to
Docker run command (Installation from Docker Hub)	Specify the argument while running the docker run command: `--scanning-policy StaticScanningOnly`	

Kubernetes DaemonSet	Add the argument in the deployment yaml: `"--scanning-policy", "StaticScanningOnly"`	dynamic scanning for images without shell.

Performing Only Static Scanning for Container Images

You can now choose to perform only static scanning for your container images. This is useful in ephemeral environments where the nodes may go offline during the launch of the image scan, causing the scanning pods to be left without a node to host them.

To perform only static scanning, specify the scanning policy argument with the appropriate value as shown below:

Sensor Deployment Method	Argument
installsensor.sh command (Binary installation)	Specify the following argument in the installsensor.sh script: `ScanningPolicy=StaticScanningOnly`
Docker run command (Installation from Docker Hub)	Specify the following command line argument while running the docker run command: `--scanning-policy StaticScanningOnly`
Kubernetes DaemonSet	Add the following argument in the deployment yaml: `"--scanning-policy", "StaticScanningOnly"`

Issues Addressed

The following issues have been fixed with this release:

- Previously, the registry sensor was unable to perform the "v2/manifests" call when a multi-architecture docker image was detected during the registry scan. The sensor now fetches and lists the image that is compatible with the host architecture from the multi-architecture image.
- The Container Security sensor installed on the CRI-O runtime recorded an inaccurate date and time for a container deletion event.