Qualys Container Security

Release Notes

Version 1.19
September 8, 2022

Here's what's new in Container Security 1.19!

SCA Scanning Now Supported

SCA Scanning Now Supported

This release brings support for Software Composition Analysis (SCA) scanning of container images. An SCA scan discovers installed open source software and libraries, as well as associated vulnerabilities, present in your container images.

While evaluating security posture of container images it is important to identify all software packages present in the image. The SCA scan can be used to identify programming language-based software packages inside the image. In addition, metadata information for each image layer is also provided. The SCA scan detects packages for these programming languages: Java, Python, Go, Node.js, .NET.

SCA scanning is supported for all sensor types – General, Registry and CI/CD. It's supported for Docker Runtime only. SCA scanning is only supported when scanning container images. SCA scanning is not supported for Mac OS.

Prerequisites

- The SCA Scanning feature must be enabled for your subscription. Contact Qualys Support to have this feature enabled.
- Update your sensors to version 1.19 or later.
- Relaunch your sensors with the parameter **--perform-sca-scan** to perform SCA scanning.

How it Works

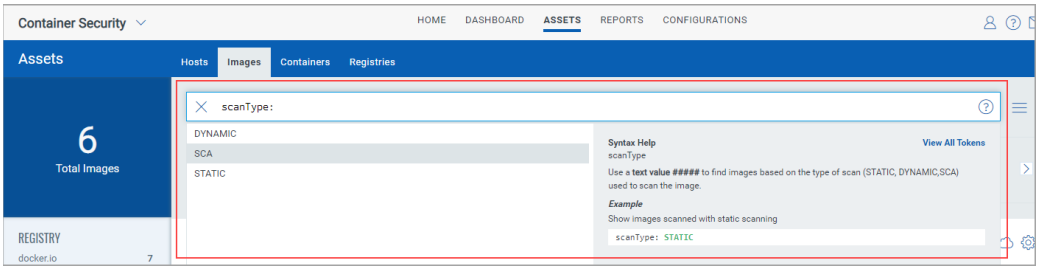
SCA scanning is not performed by default. Users must enable SCA scanning using the new parameter **--perform-sca-scan** when deploying their sensors. When enabled, an SCA scan is performed after a standard vulnerability scan (Static or Dynamic) on your container images. When the SCA scan completes, the sensor uploads the metadata information collected by the scan to the Qualys backend where posture evaluation is performed. You can view SCA scan data findings in the Container Security UI and API as part of image details. Vulnerability detections found by the SCA scan are presented as QIDs. Filters are provided so you can identify the type of scan (SCA, Dynamic or Static) used to detect a particular vulnerability.

View SCA Findings in the UI

You can view details for any image where an SCA scan has been performed to see installed software and vulnerabilities detected by the SCA scan.

Search for SCA Scanned Images

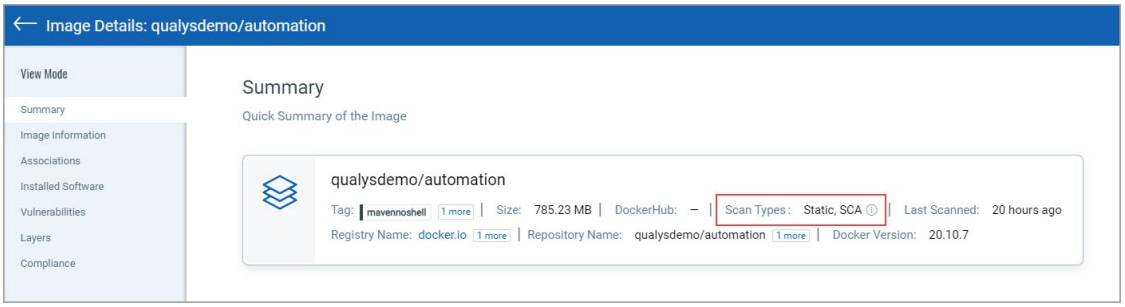
To search images, go to **Assets** > **Images**. Use **scanType** to find images based on the type of scan that was performed to scan the image. The values STATIC and DYNAMIC were previously supported. Now SCA is also supported.



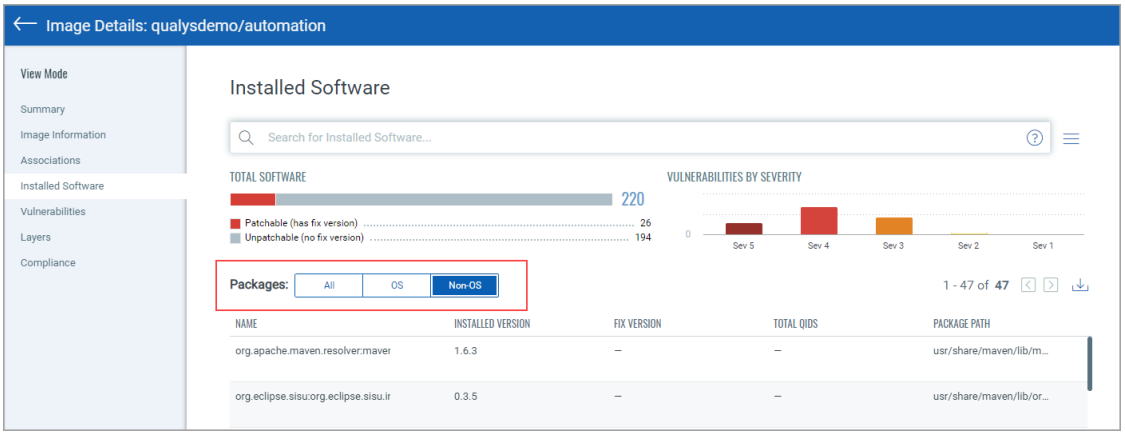
View Image Details

Go to **Assets** > **Images** and choose **View Details** for any image listed.

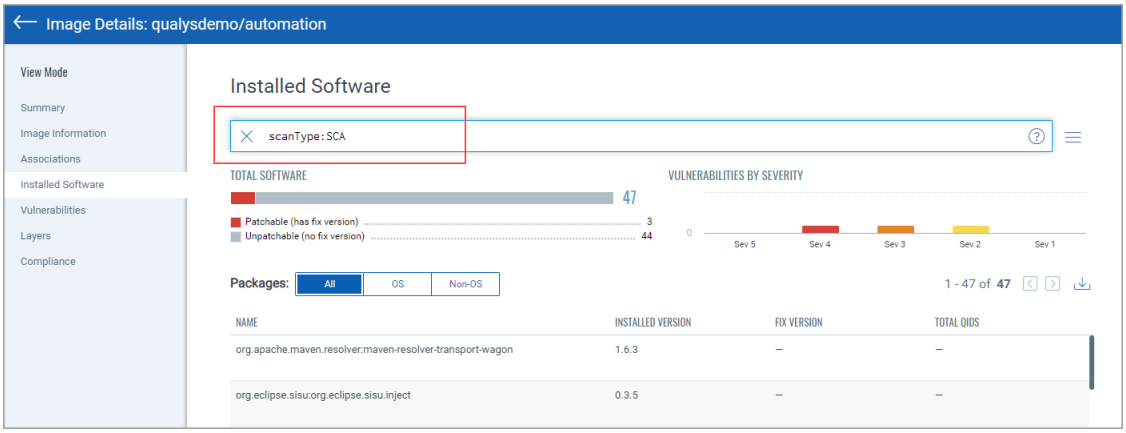
The **Summary** tab shows general information about the image. The **Scan Types** field will show the types of scans run on the image, including SCA.



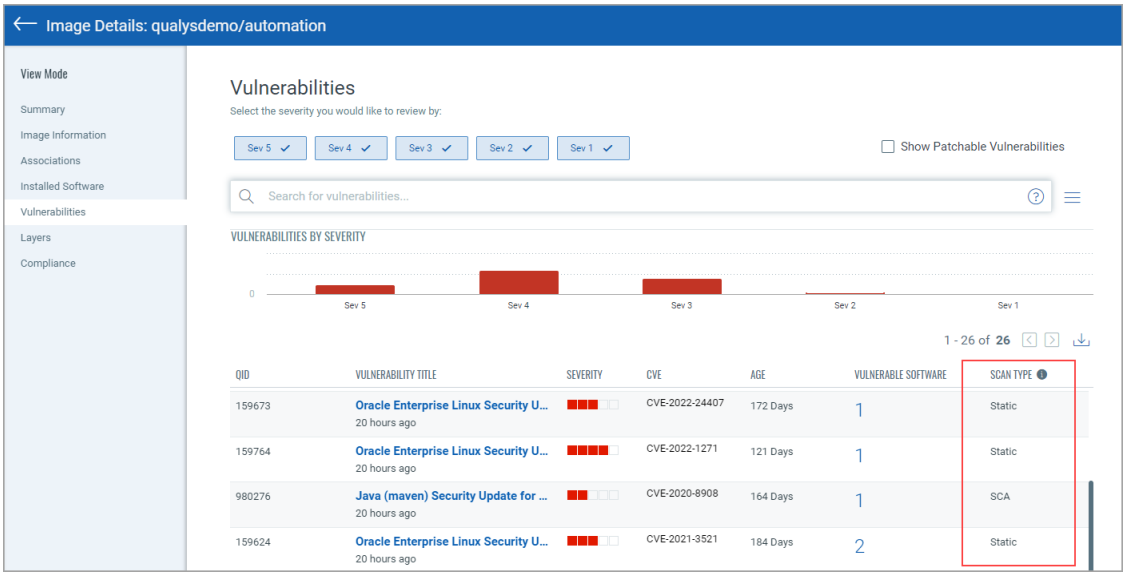
The **Installed Software** tab lists software detected by scans. Use the **Packages** filter to easily switch the list view. Choose **All** to see all software packages, choose **OS** to see only Operating System based packages, or choose **Non-OS** to see SCA related packages.



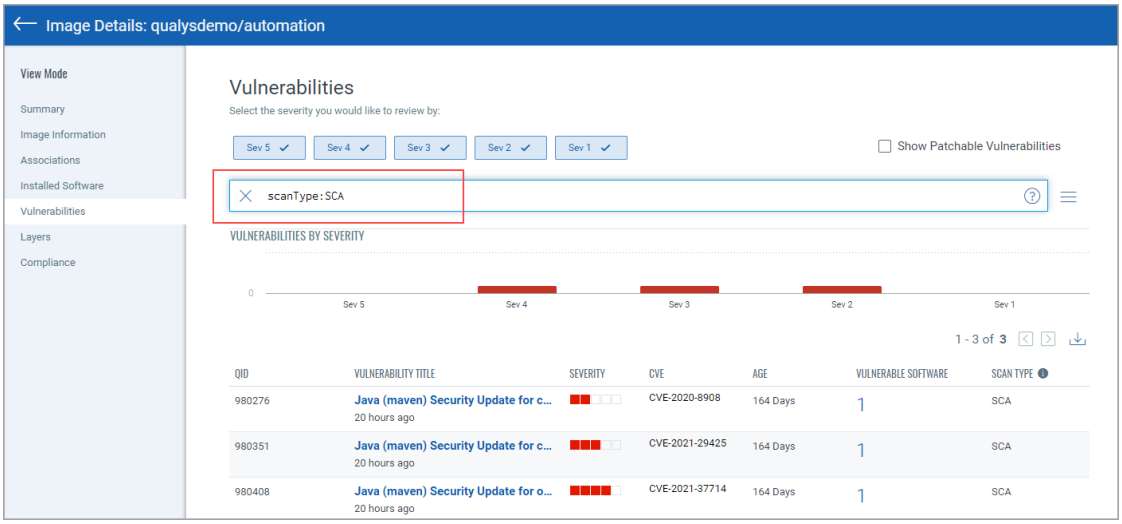
You can also search installed software detected by SCA scans using **scanType: SCA**.



The **Vulnerabilities** tab shows vulnerabilities detected by all scans, including SCA scans. This tab includes a new **SCAN TYPE** column which identifies the type of scan used for each detection.



You can also search vulnerabilities detected by SCA scans using **scanType: SCA**.



Note about Vulnerability Counts

You'll notice a difference in the number of vulnerabilities reported for an image that has been scanned by SCA and the number of vulnerabilities for the containers launched from the image. This is because the SCA scan is only run on the image, not on containers, and the SCA scan detects package based vulnerabilities. In other words, the image scan reports all vulnerabilities, including OS based vulnerabilities and Non-OS or SCA package related vulnerabilities whereas the container scan reports only the OS based vulnerabilities.

For example, let's say we scan an image using a sensor launched with the Perform SCA flag enabled and get 25 vulnerabilities reported. We launch a container on this image and it reports 22 vulnerabilities. 3 vulnerabilities were excluded because they were package based.