Container Security

Release Notes for Sensor

Version 1.10.1

December 22, 2021

Here’s what’s new in the Container Security Sensor!

Sensor Detects New Log4j Vulnerabilities

The Qualys Container Security Sensor can now detect recently released Log4j Remote Code Execution (RCE) Vulnerability QIDs. The sensor can detect the presence of vulnerable log4j packages on your container images and running containers.

See this blog post to learn more about log4j QIDs:
https://blog.qualys.com/vulnerabilities-threat-research/2021/12/10/apache-log4j2-zero-day-exploited-in-the-wild-log4shell

Want to disable log4j scanning for images?

The sensor will automatically perform a file system search to detect log4j vulnerabilities on your container images, and this can have a performance impact. To disable the log4j vulnerability scanning, specify --disable-log4j-scanning as a command line parameter for “installsensor.sh” script or provide it as a command or args parameter when deploying a sensor. See details below.

Installsensor.sh Command

Specify --disable-log4j-scanning as a command line argument for installsensor.sh script.

```
sudo ./installsensor.sh ActivationId=<Activation id> CustomerId=<Customer id>
Storage=/usr/local/qualys/sensor/data -s --disable-log4j-scanning
```

Docker Run Command

Specify --disable-log4j-scanning as part of the Docker run command when deploying a sensor.

```
sudo docker run -d --restart on-failure -v
/var/run/docker.sock:/var/run/docker.sock:ro -v
/usr/local/qualys/sensor/data:/usr/local/qualys/qpa/data -e
ACTIVATIONID=<Activation id> -e CUSTOMERID=<Customer id> -e POD_URL=<POD
URL> --net=host --name qualys-container-sensor qualys/qcs-sensor:latest
--disable-log4j-scanning
```

Yaml Argument

Add --disable-log4j-scanning argument in args section of yaml, as shown below.

```
args: ["--k8s-mode", "--disable-log4j-scanning"]
```