



Qualys Container Security v1.x

Release Notes

Version 1.3

August 7, 2018

Here's what's new in Container Security 1.3!

[Improved vulnerabilities display for images and containers](#)

[Container Security tab in Asset Details](#)

[List privileged containers](#)

[Deploying container sensor on orchestrators](#)

[Sensor upgrade information](#)

[Fixed issues](#)

Improved vulnerabilities display for images and containers

The Vulnerabilities tab in image details and container details, now displays the vulnerabilities by severity graph and list of vulnerabilities by QIDs on a single page. Select Show Patchable Vulnerabilities to view vulnerabilities with available patches.

Vulnerabilities

Select the severity you would like to review by:

Sev 5 ✓ Sev 4 ✓ Sev 3 ✓ Sev 2 ✓ Sev 1 ✓ ☐ Show Patchable Vulnerabilities

Search for vulnerabilities...

VULNERABILITIES BY SEVERITY

1 - 4 of 4

QID	VULNERABILITY TITLE	SEVERITY	CVE	VULNERABLE SOFTWARE
115284	IP Forwarding Enabled a month ago	Sev 2	CVE-1999-0511	—
370845	Linux Kernel 'drivers/scsi/libsas/sas_expander.c' ... a month ago	Sev 3	CVE-2018-7757	—
38510	CA Agent Discloses Exact Operating System Versi... a month ago	Sev 1	—	—

Click View Details from the Quick Actions Menu of a QID to view details of the vulnerability found.

Vulnerability Details: IP Forwarding Enabled

Vulnerability Summary

Severity: 2
115284
Last Found: July 25, 2018 07:04 pm

Identification	CVSS Summary	Vulnerability Analysis
QID: 115284	CVSSv2 Base: 7.5	Exploitability: 0
Category: Local	CVSSv2 Temporal: 6.8	Patches: 0
Published Date: September 29, 2005 1 2:30 pm	CVSSv3 Base: 9.8	Malwares: 0
Modified Date: —	CVSSv3 Temporal: 8.5	
Discovery Method: AUTHENTICATED	Access Vector: Network	
Authentication: UNIX_AUTH	Vendor Reference:	
Supported Apps: VM, CA-Linux Agent, C A-Mac Agent		

Threats

If this machine is not intended to be a router, then it may allow a malicious user to access your internal network.

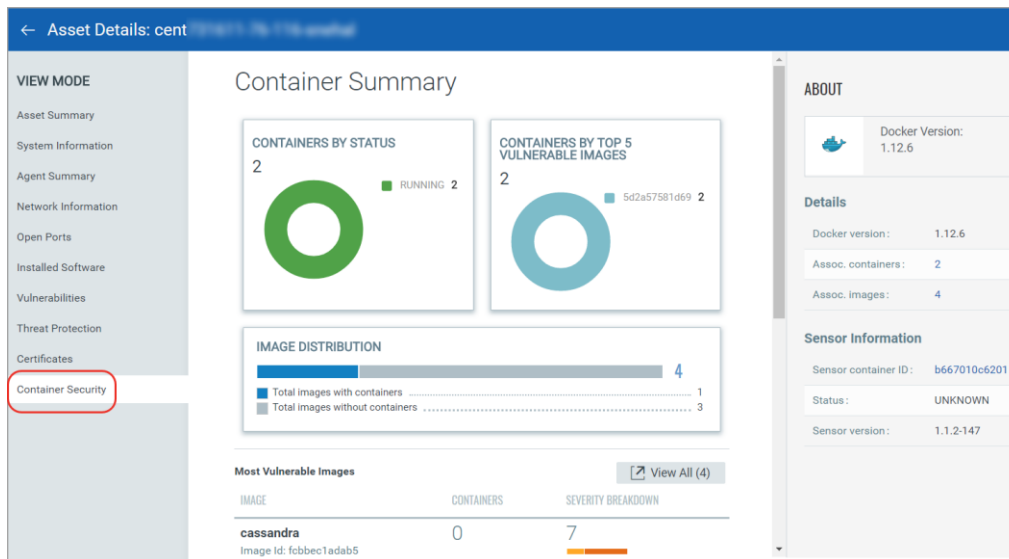
Solution

Disable IP forwarding by following the appropriate instructions below: On Windows 2000 and Windows NT, set the value of the following registry key to zero: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\IPEnableRouter On Linux, insert this line in your startup script: "sysctl -w net.ipv4.ip_forward=0" On Solaris, HP-UX B11.11 and B11.00, insert this line in your startup script: "nnd -set /dev/ip

Container Security tab in Asset Details

Asset Details now includes Container Security tab that contains information about containers installed on the host, their status, and containers with vulnerable images.

To view Asset Details, go to Containers > Sensors, and from the Quick Actions menu of a sensor, click View Host Details.



List privileged containers

You can now use the privileged filter on containers tab to list privileged containers.

Container Security ▾ DASHBOARD ASSETS EVENTS CONFIGURATIONS

Assets Images Containers

109 Total Containers

Severity 2 28
Severity 1 1

STATE
STOPPED 61
RUNNING 47
DELETED 1

ROGUE
Vulnerability 19
Software 13

PRIVILEGED
false 105
true 4

Search for containers...

CONTAINER	CREATED ON ▾	HOST	STATE
trupti3	Jun 26, 2018	dockertesting 10.115.77.151	RUNNING a month ago
trupti12	Jun 26, 2018	dockertesting 10.115.77.151	RUNNING a month ago
ubuntu1	Jun 25, 2018	dockertesting 10.115.77.151	RUNNING a month ago
optimistic_keldysh	Jun 25, 2018	dockertesting 10.115.77.151	DELETED a month ago
jolly_wescoff	Jun 20, 2018	docker1 10.115.78.111	RUNNING a month ago
thirsty_thompson	Jun 20, 2018	docker1 10.115.78.111	RUNNING a month ago
hopeful_fermat	Jun 20, 2018	docker1 10.115.78.111	RUNNING a month ago

Deploying container sensor on orchestrators

The Sensor download page now contains a link to the Container Security User Guide. The Appendix section of the user guide contains information on deploying container sensor on various orchestrators such as Kubernetes, Docker Swarm, AWS ECS Cluster, and Mesosphere DC/OS.

Once you launch the sensor download page from the Configurations> Sensors tab, click More Instructions to get the link to the user guide.

Copy and paste

```
sudo tar -xvf QualysContainerSensor.tar.xz
```

```
sudo mkdir -p /usr/local/qualys/sensor/data
```

```
sudo ./installsensor.sh ActivationId=3c8e5c58-614e-4d31-8360-6f5d39df3438 CustomerId=84c725a5-c071-6021-82f6 Storage=/usr/local/qualys/sensor/data -s
```

[Hide Instructions](#)

Instructions

ActivationId: Activation Id for the container sensor, auto-generated based on your subscription.

CustomerId: Qualys subscription's customerId, auto-generated based on your subscription.

Storage: Directory where the sensor would store the files. Recommended: /usr/local/qualys/sensor/data, create it if no can specify a custom directory location (provided that it exists).

ImageFile: Location of the sensor ImageFile, defaults to the local directory. [optional]

LogLevel: Configuration to set the logging level for sensor, accepts 0 to 5. [optional]

HostIdSearchDir: Directory to map the marker files created by Qualys Agent or Scanner appliance on the host, update if

ConcurrentImageScan: Number of concurrent images scan thread pool size. [optional]

ConcurrentContScan: Number of concurrent containers scan thread pool size. [optional]

Proxy: IPv4/IPv6 address or FQDN of the proxy server. [optional]

ProxyCertFile: Proxy certificate file path. [optional]

Deploy sensor containers on Kubernetes and AWS ECS environments, [click here to learn more.](#)

Sensor upgrade information

The [Container Security User Guide](#) now contains information about sensor upgrade. See section “Sensor updates”. For information about sensor crash or restart, see sections “Sensor crashes during upgrade” and “What if sensor restarts?”.

Fixed issues

The following issue is fixed in release 1.3.

Fixed an issue where downloading a report for Containers was failing when search query used was in the following format:
`vulnerabilities.severity:"Severity 5"`