

The background features a series of concentric circles in light gray, some solid and some dashed, creating a ripple effect. A large green speech bubble is centered on the page, containing the text 'Container security'.

# Container security

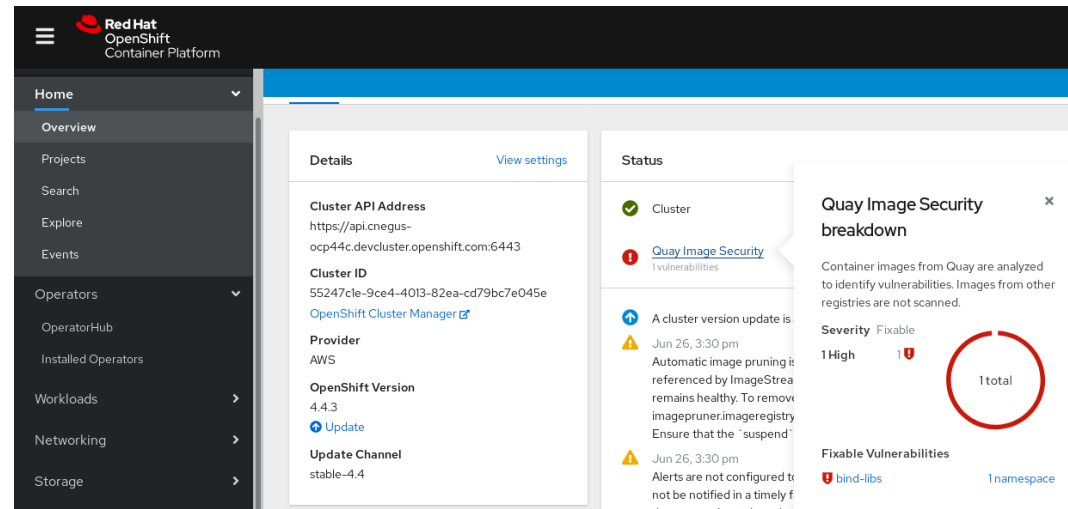
# Danger of vulnerabilities

- Image vulnerabilities
  - For example: using an untrusted base image in your Dockerfile, you'd be exposing yourself to vulnerable system libraries bundled with the image.
- Vulnerabilities in system libraries
  - In 2018 alone 1,597 vulnerabilities in system libraries were tracked with known CVEs assigned, which is more than four times the number of vulnerabilities compared to 2017
  - Year over year high and critical vulnerabilities number is growing

## Container Security using Red Hat Quay with Clair

- Red Hat Quay is a distributed and highly available container image registry
- Red Hat Quay supports scanning container images for known vulnerabilities with a scanning engine such as Clair
- Clair provides a tool to monitor the security of your containers through the static analysis of vulnerabilities in applications and docker containers.
- Clair is an API-driven analysis engine that inspects containers layer-by-layer for known security flaws.
- Using Clair, you can easily build services that provide continuous monitoring for container vulnerabilities.
- Available as part of OpenShift Platform Plus

# Demo



The screenshot shows the Red Hat OpenShift Container Platform dashboard. The left sidebar contains navigation links: Home, Overview, Projects, Search, Explore, Events, Operators (with sub-links for OperatorHub and Installed Operators), Workloads, Networking, and Storage. The main content area is divided into three sections: Details, Status, and a Quay Image Security breakdown. The Details section shows cluster information: Cluster API Address (https://api.cnegus-ocp44c.devcluster.openshift.com:6443), Cluster ID (55247cle-9ce4-4013-82ea-cd79bc7e045e), Provider (AWS), OpenShift Version (4.4.3), and Update Channel (stable-4.4). The Status section shows a green checkmark for the Cluster and a red exclamation mark for Quay Image Security. The Quay Image Security breakdown shows a donut chart with 1 total vulnerability, 1 High severity, and 1 Fixable Vulnerability (bind-libs).

**Red Hat OpenShift Container Platform**

**Details** [View settings](#)

**Cluster API Address**  
https://api.cnegus-ocp44c.devcluster.openshift.com:6443

**Cluster ID**  
55247cle-9ce4-4013-82ea-cd79bc7e045e  
[OpenShift Cluster Manager](#)

**Provider**  
AWS

**OpenShift Version**  
4.4.3  
[Update](#)

**Update Channel**  
stable-4.4

**Status**

- Cluster
- Quay Image Security**  
1 vulnerabilities
- A cluster version update is available. Automatic image pruning is referenced by ImageStream remains healthy. To remove imagepruner.imageregistry Ensure that the "suspend" Alerts are not configured to not be notified in a timely f

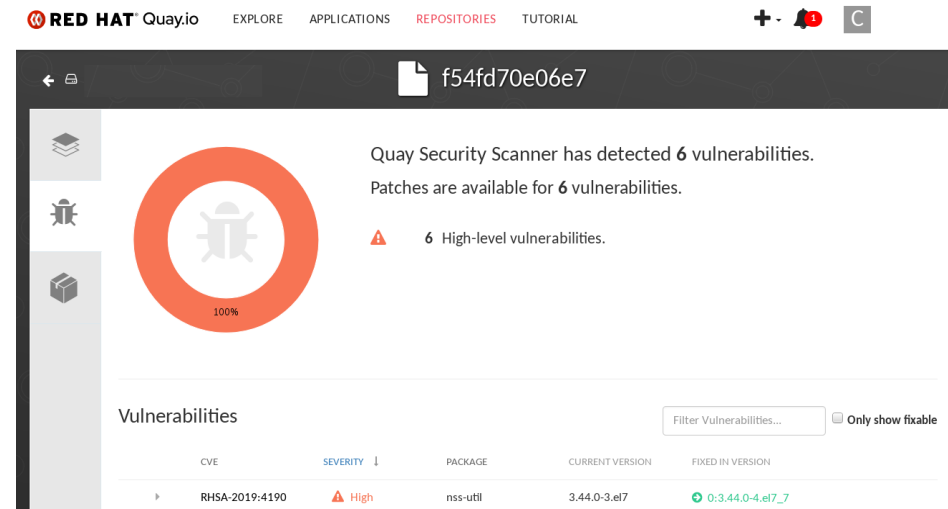
**Quay Image Security breakdown**

Container images from Quay are analyzed to identify vulnerabilities. Images from other registries are not scanned.

**Severity** Fixable  
1 High 1

**1 total**

**Fixable Vulnerabilities**  
1 bind-libs 1 namespace



The screenshot shows the Red Hat Quay.io interface. The top navigation bar includes links for EXPLORE, APPLICATIONS, REPOSITORIES, and TUTORIAL. The main content area shows a repository named f54fd70e06e7. A donut chart indicates that 100% of the vulnerabilities are fixable. The text states: "Quay Security Scanner has detected 6 vulnerabilities. Patches are available for 6 vulnerabilities." Below this, it says "6 High-level vulnerabilities." The Vulnerabilities table lists the following data:

CVE	SEVERITY	PACKAGE	CURRENT VERSION	FIXED IN VERSION
RHSA-2019-4190	High	nss-util	3.44.0-3.el7	0:3.44.0-4.el7_7

## Further information

- <https://developers.redhat.com/blog/2019/06/26/using-quay-io-to-find-vulnerabilities-in-your-container-images>
- [https://access.redhat.com/documentation/en-us/red\\_hat\\_quay/2.9/html/manage\\_red\\_hat\\_quay/quay-security-scanner](https://access.redhat.com/documentation/en-us/red_hat_quay/2.9/html/manage_red_hat_quay/quay-security-scanner)
- <https://docs.openshift.com/container-platform/4.9/security/pod-vulnerability-scan.html>