RedLock

ADVISORY: Sensitive Information Exposed via Images Shared on Docker Hub

Date Published: July 18, 2017

Issue Summary

The RedLock CSI team found that many organizations have accidentally shared internal Docker images publicly.

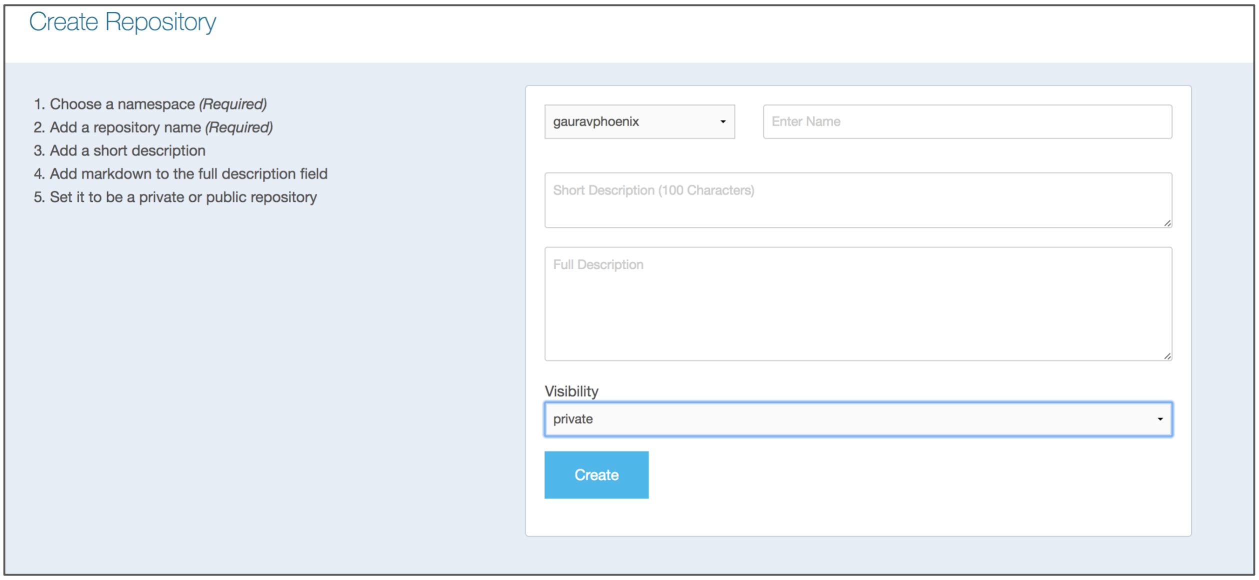
The Impact

The misconfiguration has led to the exposure of source code and other sensitive information.

Background

Docker Hub repositories let you share images with co-workers, customers, or the Docker community at large. If you're building your images internally, either on your own Docker daemon, or using your own continuous integration services, you can push them to a Docker Hub repository that you add to your Docker Hub user or organization account.

When creating a repository, changing the "Visibility" drop down field enables you to make an image public or private. Many organizations have accidentally set this field to "public", exposing source code and other sensitive information.



Create Repository

1. Choose a namespace *(Required)*
2. Add a repository name *(Required)*
3. Add a short description
4. Add markdown to the full description field
5. Set it to be a private or public repository

gauravphoenix

Visibility: private

Figure 1: **The "Visibility" drop down field makes an image public or private**

Remediation

1. Performing a simple search such as the one below with your **organization's or business unit's names** might identify some images that are publicly exposed: https://hub.docker.com/search/?isAutomated=0&isOfficial=0&page=1&pullCount=0&q=mycompany&starCount=0
2. Train developers on security best practices, and educate them on the implications of inadvertently sharing internal Docker images.

About RedLock

RedLock enables organizations to accelerate digital business by managing security and compliance risks within their public cloud infrastructure. It provides the most comprehensive view of cloud computing environments, even across multiple public cloud service providers. The RedLock Cloud 360™ platform supports cloud forensics, policy monitoring, anomaly detection, contextual alerting, and compliance reporting, all to deliver unparalleled true cloud infrastructure security without impeding DevOps.

The RedLock Cloud Security Intelligence (CSI) team consists of elite security analysts, data scientists, and data engineers with deep enterprise security expertise. The team's mission is to enable organizations to confidently adopt public cloud infrastructure by researching cloud threats, advising organizations on cloud security best practices, and frequently publishing out-of-the-box policies in the RedLock Cloud 360 platform.

Trademarks

RedLock, RedLock logo, and RedLock Cloud 360 are trademarks of RedLock Inc. All other registered trademarks are the properties of their respective owners.