

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 7

Scenario : Securing a Docker Image Before Deployment to Production

John, a developer, is working on a web application called SecureApp that his team plans to deploy to a Kubernetes cluster in IBM Cloud. Before deployment, John wants to ensure the Docker image for SecureApp is secure and free from vulnerabilities. He decides to use IBM Cloud Container Registry and Vulnerability Advisor to scan the image for security issues and make the necessary corrections.

Steps :

- **Building the Docker Image**
- **Tag the image for container registry**
- **Login to IBM Cloud Container Registry**
- **Push Image to Container Registry**
- **Check Vulnerability Scan Results**
- **Address Vulnerabilities**
- **Rebuild and Re-scan the Image**
- **Deploy the Secure Image**

Steps and Screenshots :

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA Batch - 71

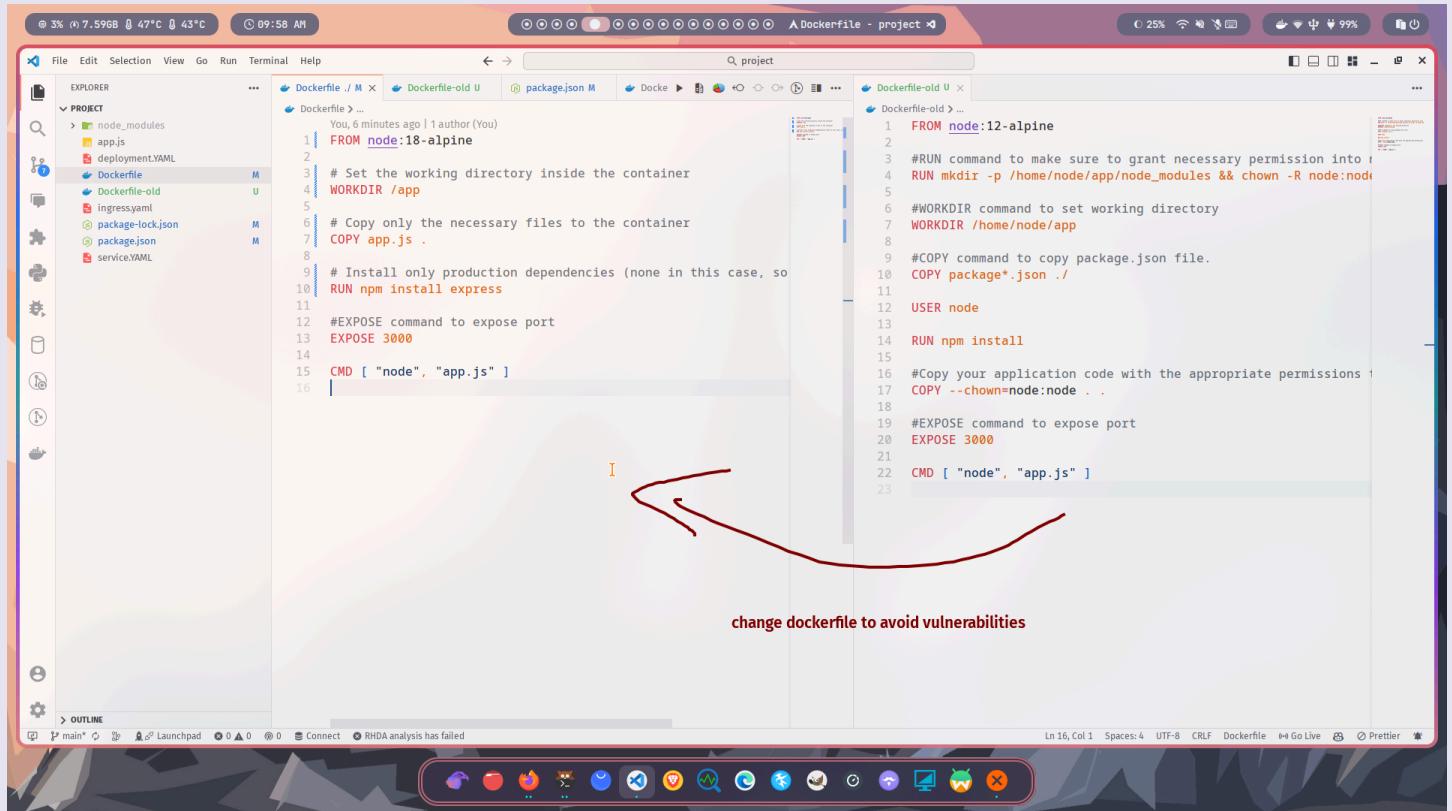
CS Practical 7

1. Use previously created image on IBM Container Registry and scan the vulnerabilities

The screenshot shows the IBM Cloud Container Registry interface. On the left, there's a sidebar with 'Image details' and 'Issues by type' selected. The main area is titled 'Overview' and features a warning icon with 'Do not deploy' text, a shield icon with '12 vulnerabilities', and a gear icon with '0 configuration issues'. Below this, under 'Vulnerabilities', it says 'Vulnerability Advisor checks your images for known vulnerabilities based on official community maintained lists.' A link to 'Learn more' is provided. A table lists vulnerabilities, with one entry for CVE-2023-3817: 'Affected packages' (libssl1.1, libcrypto1.1) and 'How to resolve' (Upgrade 2 packages). Another section, 'Summary', shows vendor security notice IDs for CVE-2023-3817 (ALPINE-CVE-2023-3817) and affected packages (libssl1.1, libcrypto1.1) with their respective policy status (Active) and how to resolve (Upgrade libssl1.1 to >= 1.1.1v-r0, Upgrade libcrypto1.1 to >= 1.1.1v-r0). At the bottom, there's a toolbar with various icons.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 7

2. Modify Dockerfile to solve issues



The screenshot shows a code editor interface with two Dockerfiles side-by-side. On the left is the 'Dockerfile' file, and on the right is the 'Dockerfile-old' file. A red arrow points from the left Dockerfile towards the right one.

Dockerfile (Left):

```
1 FROM node:18-alpine
2
3 # Set the working directory inside the container
4 WORKDIR /app
5
6 # Copy only the necessary files to the container
7 COPY app.js .
8
9 # Install only production dependencies (none in this case, so
10 RUN npm install express
11
12 #EXPOSE command to expose port
13 EXPOSE 3000
14
15 CMD [ "node", "app.js" ]
16
```

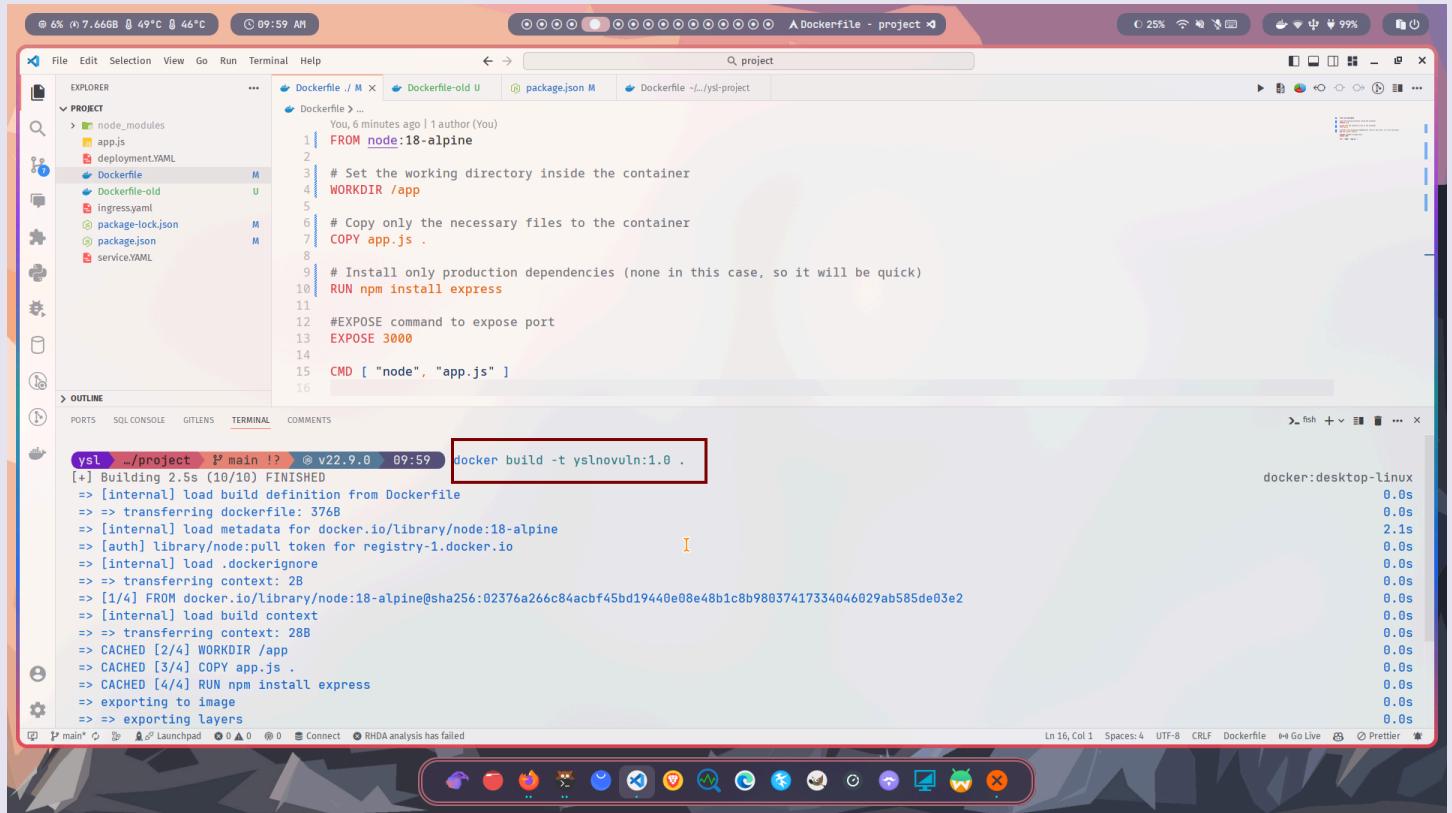
Dockerfile-old (Right):

```
1 FROM node:12-alpine
2
3 #RUN command to make sure to grant necessary permission into !
4 RUN mkdir -p /home/node/app/node_modules && chown -R node:node .
5
6 #WORKDIR command to set working directory
7 WORKDIR /home/node/app
8
9 #COPY command to copy package.json file.
10 COPY package*.json .
11
12 USER node
13
14 RUN npm install
15
16 #Copy your application code with the appropriate permissions !
17 COPY --chown=node:node .
18
19 #EXPOSE command to expose port
20 EXPOSE 3000
21
22 CMD [ "node", "app.js" ]
23
```

change dockerfile to avoid vulnerabilities

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 7

3. Build image



The screenshot shows a terminal window within a code editor interface. The terminal is running a Docker build command:

```
ysl ~/project $ docker build -t yslnovuln:1.0 .
```

The output of the command is displayed in the terminal window:

```
[+] Building 2.5s (10/10) FINISHED
=> [internal] load build definition from Dockerfile
=> transferring dockerfile: 376B
=> [internal] load metadata for docker.io/library/node:18-alpine
=> [auth] library/node:pull token for registry-1.docker.io
=> [internal] load .dockerrcignore
=> transferring context: 2B
=> [1/4] FROM docker.io/library/node:18-alpine@sha256:02376a266c84acbf45bd19440e08e48b1c8b98037417334046029ab585de03e2
=> [internal] load build context
=> transferring context: 28B
=> CACHED [2/4] WORKDIR /app
=> CACHED [3/4] COPY app.js .
=> CACHED [4/4] RUN npm install express
=> exporting to image
=> exporting layers
```

On the right side of the terminal window, there is a progress bar for the Docker build process, showing the following metrics:

Step	Time
[internal] load build definition from Dockerfile	0.0s
[internal] load metadata for docker.io/library/node:18-alpine	2.1s
[auth] library/node:pull token for registry-1.docker.io	0.0s
[internal] load .dockerrcignore	0.0s
[internal] load build context	0.0s
FROM docker.io/library/node:18-alpine@sha256:02376a266c84acbf45bd19440e08e48b1c8b98037417334046029ab585de03e2	0.0s
exporting to image	0.0s
exporting layers	0.0s

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 7

4. Tag and upload to Container Registry

The screenshot shows a terminal window within a code editor interface. The terminal tab is active, displaying the following Dockerfile content:

```
FROM node:18-alpine
WORKDIR /app
COPY app.js .
RUN npm install express
EXPOSE 3000
CMD [ "node", "app.js" ]
```

Below the Dockerfile, the terminal shows a series of build logs:

```
e9879eac8a05: Preparing
22592a090fb1: Preparing
e2be10e97665: Preparing
06fd85419b65: Preparing
f58c462fa079: Waiting
63ca1fbb43ae: Waiting
denied: Your account has exceeded its image storage quota for the current month. See https://cloud.ibm.com/docs/Registry?topic=Registry-troubleshoot-quota
```

The user then runs the command:

```
ibmcloud cr region-set us-south
```

The response indicates the region is set to 'us-south' and the registry is 'us.icr.io'. A red box highlights this command.

At the bottom of the terminal window, there is a status bar with various icons and text indicating the current session details.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 7

The screenshot shows a terminal window with the following command history:

```
06fd85419b65: Preparing
f58c462fa079: Waiting
63ca1fbba43ae: Waiting
denied: Your account has exceeded its image storage quota for the current month. See https://cloud.ibm.com/docs/Registry?topic=Registry-troubleshoot-quota

y whole project 1 main !? @ v22.9.0 10:06 ibmcloud cr region-set us-south
The region is set to 'us-south', the registry is 'us.icr.io'.
```

OK

```
y whole project 1 main !? @ v22.9.0 10:09 ibmcloud cr login
Logging "docker" in to "us.icr.io"...
Logged in to "us.icr.io".
```

OK

```
y whole project 1 main !? @ v22.9.0 10:09
```

The screenshot shows a terminal window with the following command history:

```
No resource group is targeted. Therefore, the default resource group for the account ('default') is targeted.

Adding namespace 'yashlani-nmspc' in resource group 'default' for account IBM India Pvt Ltd, C/o Software in registry us.icr.io...
Successfully added namespace 'yashlani-nmspc'

OK
```

```
y whole project 1 main !? @ v22.9.0 10:11
```

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 7

The screenshot shows a terminal window with the following command history:

```
Successfully added namespace 'yashlani-nmspc'
OK
y whole-project P main !? @ v22.9.0 10:11 docker tag yslnovuln:1.0 us.icr.io/yashlani-nmspc/yslnewimage:2.0
y whole-project P main !? @ v22.9.0 10:11 docker push us.icr.io/yashlani-nmspc/yslnewimage:2.0
```

The push command is highlighted with a red box.

The screenshot shows a terminal window with the following command history:

```
OK
y whole-project P main !? @ v22.9.0 10:11 docker tag yslnovuln:1.0 us.icr.io/yashlani-nmspc/yslnewimage:2.0
y whole-project P main !? @ v22.9.0 10:11 docker push us.icr.io/yashlani-nmspc/yslnewimage:2.0
```

The push command is highlighted with a red box.

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA Batch - 71

CS Practical 7

5. Now, check results of scan, no issues should be found

The screenshot shows the IBM Cloud Container Registry interface. The URL in the address bar is <https://cloud.ibm.com/containers/registry/images/eyjyZXBvIjoidXMuaWNyLmlvL3lh2hsYW5pLW5tc3BjL3zbG5ld2ltYWdliwibG9uZ0RpZ2VzdCI6I>. The page displays the results of a scan for the image `us.icr.io/yashlani-nmspc/yslnewimage@sha256:25b731cde7883b7a90b65f2260f1446511512cf748c0ed35e82`. The interface includes sections for **Image details**, **Overview** (with a green checkmark icon), **Safe to deploy**, **Vulnerabilities** (0 vulnerabilities), and **Configuration issues** (0 configuration issues). A table titled "Vulnerabilities" is present but empty. The bottom navigation bar features various icons for different services like Cloud Functions, Watson Assistant, Watson Studio, and Watson Machine Learning.

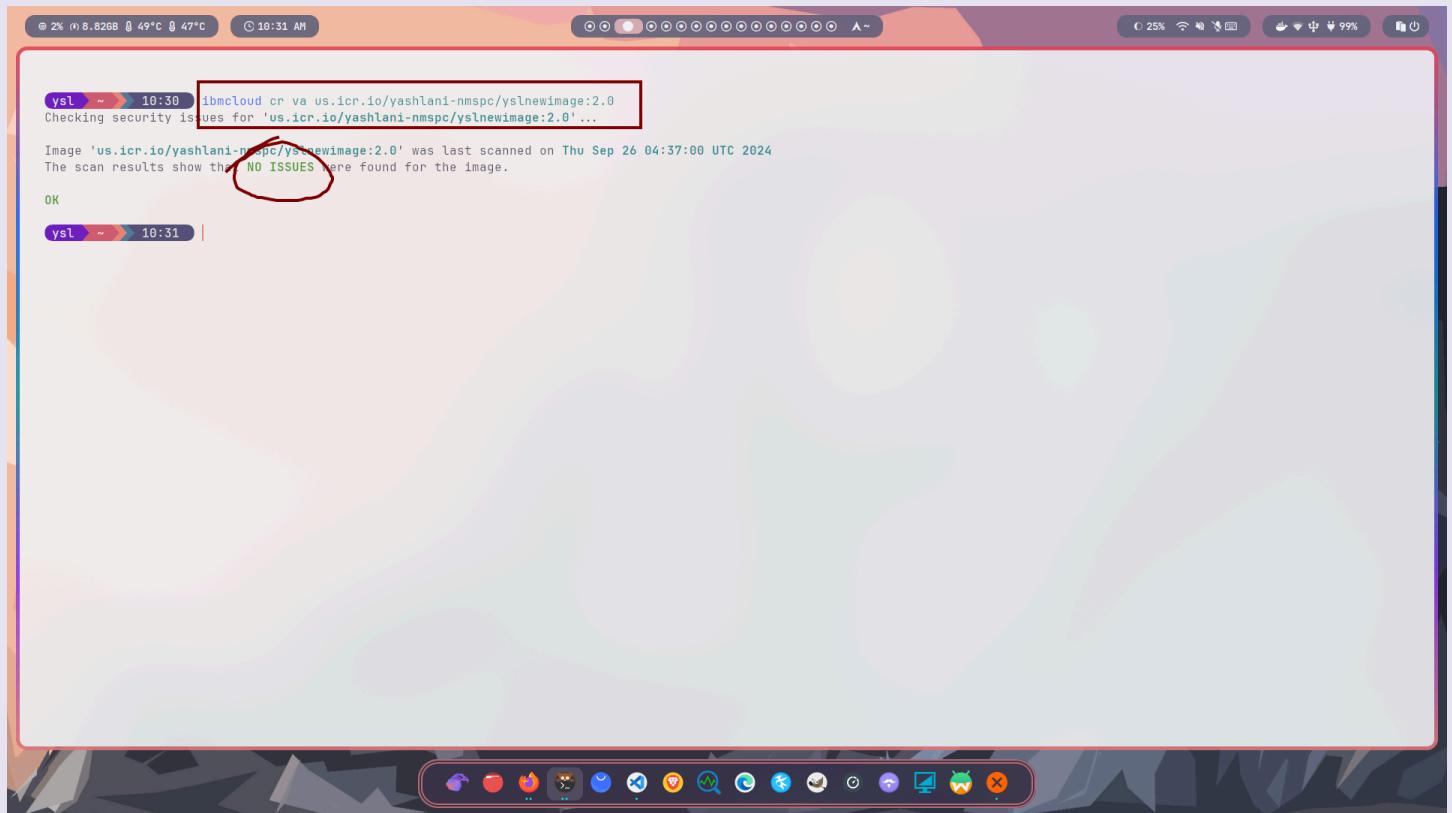
Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA Batch - 71

CS Practical 7

6. Also, it can be checked using cli



The screenshot shows a terminal window with a light gray background and a dark blue header bar. The header bar includes system status icons like battery level (2%), signal strength, and temperature (49°C). The main terminal area has a red border around the command line. The command entered is:

```
ibmcloud cr va us.icr.io/yashlani-nmspc/yslnewimage:2.0
```

Below the command, the output shows:

```
Checking security issues for 'us.icr.io/yashlani-nmspc/yslnewimage:2.0'...
```

Image 'us.icr.io/yashlani-nmspc/yslnewimage:2.0' was last scanned on Thu Sep 26 04:37:00 UTC 2024
The scan results show that NO ISSUES were found for the image.

OK

At the bottom of the terminal window, there is a dock with various application icons, including a browser, file manager, terminal, and system tray.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 7

```
ysl ~ 10:32 ibmcloud cr va au.icr.io/yashlani-nmspc/yslnewimage:1.0
FAILED
The supplied image name 'au.icr.io/yashlani-nmspc/yslnewimage:1.0' doesn't match the targeted registry 'us.icr.io'.
Correct the image name, or use 'ibmcloud cr region-set' to target the correct registry, and try again.

ysl ~ 10:32 ibmcloud cr region-set au-syd
The region is set to 'ap-south', the registry is 'au.icr.io'.

OK

ysl ~ 10:33 ibmcloud cr va au.icr.io/yashlani-nmspc/yslnewimage:1.0
Checking security issues for 'au.icr.io/yashlani-nmspc/yslnewimage:1.0'...

old image with issues

Image 'au.icr.io/yashlani-nmspc/yslnewimage:1.0' was last scanned on Thu Sep 26 03:44:23 UTC 2024
The scan results show that 12 ISSUES were found for the image.

Vulnerable Packages Found
=====
Vulnerability ID Policy Status Affected Packages How to Resolve
CVE-2023-3817 Active libss1.1 and libcrypto1.1 Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-2650 Active libss1.1 and libcrypto1.1 Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-0215 Active libss1.1 and libcrypto1.1 Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-3446 Active libss1.1 and libcrypto1.1 Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-0465 Active libss1.1 and libcrypto1.1 Upgrade 2 packages. Re-run command with --extended to view.
CVE-2022-4450 Active libss1.1 and libcrypto1.1 Upgrade 2 packages. Re-run command with --extended to view.
CVE-2022-4304 Active libss1.1 and libcrypto1.1 Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-0464 Active libss1.1 and libcrypto1.1 Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-0286 Active libss1.1 and libcrypto1.1 Upgrade 2 packages. Re-run command with --extended to view.
CVE-2022-2097 Active libss1.1 and libcrypto1.1 Upgrade 2 packages. Re-run command with --extended to view.
CVE-2023-5678 Active libss1.1 and libcrypto1.1 Upgrade 2 packages. Re-run command with --extended to view.
CVE-2022-37434 Active zlib Upgrade zlib to ≥ 1.2.12-r2

To see the details about the fixes for these packages, run the command again with the '--extended' flag.

OK

ysl ~ 10:33 |
```

```
OK

ysl ~ 10:40 ibmcloud cr va au.icr.io/yashlani-nmspc/yslnewimage:1.0 --extended
Checking security issues for 'au.icr.io/yashlani-nmspc/yslnewimage:1.0'...

Image 'au.icr.io/yashlani-nmspc/yslnewimage:1.0' was last scanned on Thu Sep 26 03:44:23 UTC 2024
The scan results show that 12 ISSUES were found for the image.

Vulnerable Packages Found
=====
CVE-2023-3817
Policy Status
Active

Summary
I

Vendor Security Notice IDs Official Notice
ALPINE-CVE-2023-3817 https://www.cve.org/CVERecord?id=CVE-2023-3817

Affected Packages Policy Status How to Resolve Security Notice
libss1.1 Active Upgrade libss1.1 to ≥ 1.1.1v-r0 ALPINE-CVE-2023-3817
libcrypto1.1 Active Upgrade libcrypto1.1 to ≥ 1.1.1v-r0 ALPINE-CVE-2023-3817

CVE-2023-2650
Policy Status
Active

Summary
I

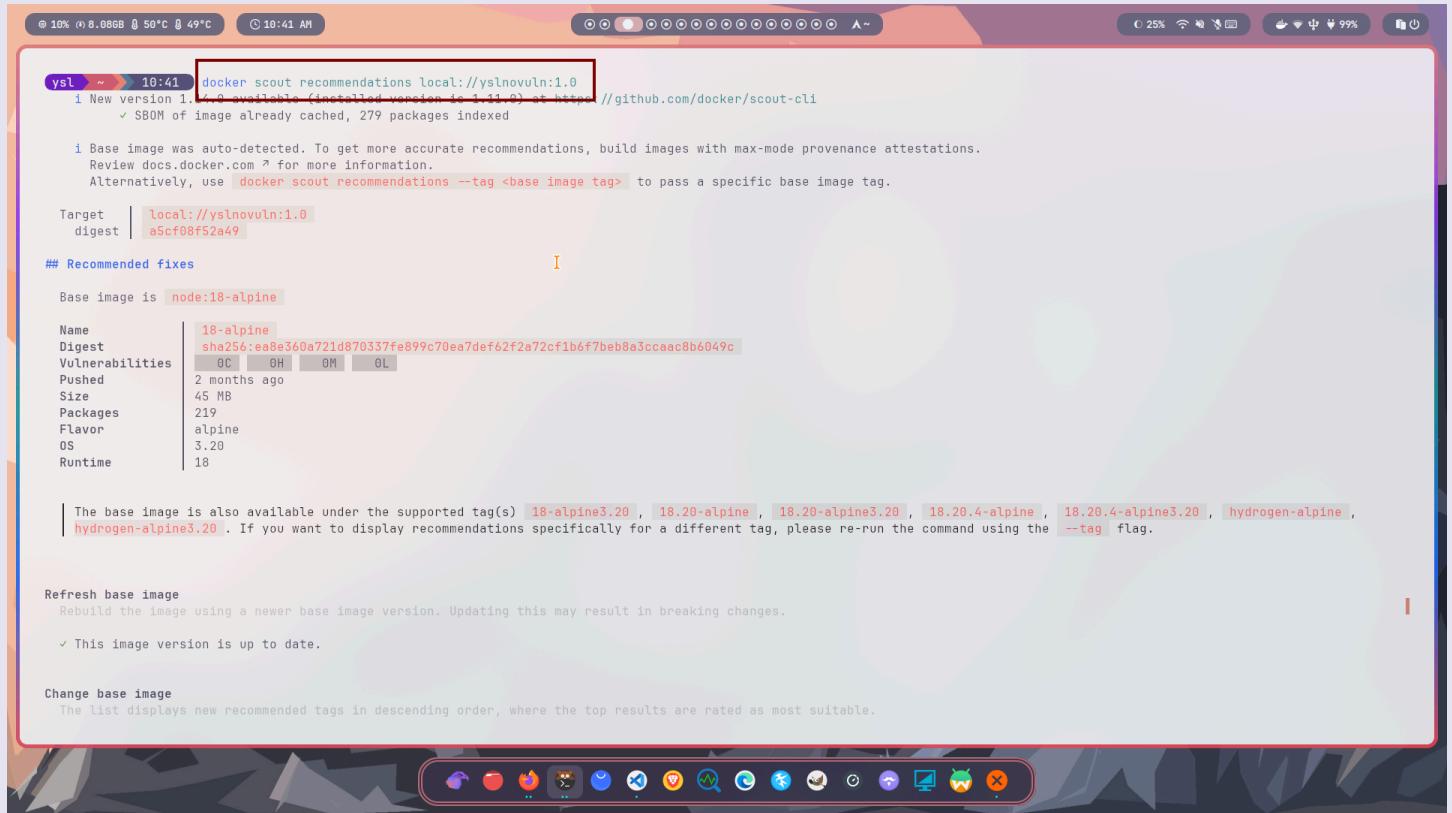
Vendor Security Notice IDs Official Notice
ALPINE-CVE-2023-2650 https://www.cve.org/CVERecord?id=CVE-2023-2650

Affected Packages Policy Status How to Resolve Security Notice
```

extended view

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 7

7. Also, docker has its own component, SCOUT to check vulnerability



```
ysl ~ 10:41 docker scout recommendations local://yslnovuln:1.0
i New version 1.1.0 available (installed version is 1.1.0) at https://github.com/docker/scout-cli
  ✓ SBOM of image already cached, 279 packages indexed

i Base image was auto-detected. To get more accurate recommendations, build images with max-mode provenance attestations.
  Review docs.docker.com ? for more information.
  Alternatively, use docker scout recommendations --tag <base image tag> to pass a specific base image tag.

Target | local://yslnovuln:1.0
digest | a5cf08f52a49

## Recommended fixes

Base image is node:18-alpine

Name          18-alpine
Digest        sha256:ea8e360a721d870337fe899c70ea7def62f2a72cf1b6f7beb8a3ccaaac8b6049c
Vulnerabilities  0C OH OM OL
Pushed        2 months ago
Size          45 MB
Packages      219
Flavor         alpine
OS             3.20
Runtime        18

The base image is also available under the supported tag(s) 18-alpine3.20 , 18.20-alpine , 18.20-alpine3.20 , 18.20.4-alpine , 18.20.4-alpine3.20 , hydrogen-alpine , hydrogen-alpine3.20 . If you want to display recommendations specifically for a different tag, please re-run the command using the --tag flag.

Refresh base image
Rebuild the image using a newer base image version. Updating this may result in breaking changes.

✓ This image version is up to date.

Change base image
The list displays new recommended tags in descending order, where the top results are rated as most suitable.
```

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 7

Target | local://yslnovuln:1.0
digest | a5cf08f52a49

Recommended fixes

Base image is node:18-alpine

Name	18-alpine
Digest	sha256:eab360a721d870337fe899c70ea7def62f2a72cf1b6f7beb8a3ccaa8b6049c
Vulnerabilities	0C OH OM OL
Pushed	2 months ago
Size	45 MB
Packages	219
Flavor	alpine
OS	3.20
Runtime	18

The base image is also available under the supported tag(s) 18-alpine3.20 , 18.20-alpine , 18.20-alpine3.20 , 18.20.4-alpine , 18.20.4-alpine3.20 , hydrogen-alpine , hydrogen-alpine3.20 . If you want to display recommendations specifically for a different tag, please re-run the command using the --tag flag.

Refresh base image

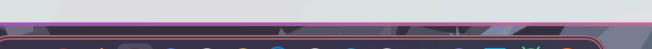
This image version is up to date, meaning a newer base image version. Updating this may result in breaking changes.

✓ This image version is up to date.

Change base image

The list displays new recommended tags in descending order, where the top results are rated as most suitable.

Tag	Details	Pushed	Vulnerabilities
22-alpine Major runtime version update Also known as: <ul style="list-style-type: none">alpine	Benefits: <ul style="list-style-type: none">Same OS detectedImage contains 6 fewer packagesMajor runtime version update	1 week ago	0C OH OM OL



Tag	Details	Pushed	Vulnerabilities
22-alpine Major runtime version update Also known as: <ul style="list-style-type: none">alpinealpine3.2022.9.0-alpine22.9.0-alpine3.2022.9-alpine22.9-alpine3.20current-alpinecurrent-alpine3.2022-alpine3.20	<p>Benefits:</p> <ul style="list-style-type: none">Same OS detectedImage contains 6 fewer packagesMajor runtime version updateTag was pushed more recentlyImage has similar sizeImage has same number of vulnerabilities <p>Image details:</p> <ul style="list-style-type: none">Size: 54 MBFlavor: alpineOS: 3.20Runtime: 22	1 week ago	0C 0H 0M 0L
20-alpine Major runtime version update Also known as: <ul style="list-style-type: none">20.17.0-alpine20.17.0-alpine3.2020.17-alpine20.17-alpine3.20lts-alpineiron-alpinelts-alpine3.20iron-alpine3.2020-alpine3.20	<p>Benefits:</p> <ul style="list-style-type: none">Same OS detectedImage contains 5 fewer packagesMajor runtime version updateTag was pushed more recentlyImage has similar sizeImage has same number of vulnerabilities <p>Image details:</p> <ul style="list-style-type: none">Size: 47 MBFlavor: alpineOS: 3.20Runtime: 20.17.0	1 month ago	0C 0H 0M 0L
slim Tag is preferred tag Also known as: <ul style="list-style-type: none">22.9.0-slim	<p>Benefits:</p> <ul style="list-style-type: none">Tag is preferred tagMajor runtime version updateTag was pushed more recently	1 week ago	0C 0H 0M 23L +23

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA Batch - 71

CS Practical 7

The screenshot shows a terminal window on a Mac OS X desktop. The terminal title is 'ysh ~ 10:41'. The command run is 'docker scout recommendations us.icr.io/yashlani-nmspc/yslnewimage:2.0'. The output includes:

- New version 1.14.0 available (installed version is 1.11.0) at <https://github.com/docker/scout-cli>
- SBOM of image already cached, 279 packages indexed
- Base image was auto-detected. To get more accurate recommendations, build images with max-mode provenance attestations. Review [docs.docker.com](#) for more information.
- Alternatively, use `docker scout recommendations --tag <base image tag>` to pass a specific base image tag.

Target: `us.icr.io/yashlani-nmspc/yslnewimage:2.0`
Digest: `a5cf08f52a49`

Recommended fixes

Base image is	<code>node:18-alpine</code>
Name	<code>18-alpine</code>
Digest	<code>sha256:ea8e360a721d870337fe899c70ea7def62f2a72cf1b6f7beb8a3ccaac8b6049c</code>
Vulnerabilities	0C OH OM OL
Pushed	2 months ago
Size	45 MB
Packages	219
Flavor	alpine
OS	3.20
Runtime	18

The image on IBM Cloud Container Registry can also be scanned by docker scout

The base image is also available under the supported tag(s) `18-alpine3.20`, `18.20-alpine`, `18.20-alpine3.20`, `18.20.4-alpine`, `18.20.4-alpine3.20`, `hydrogen-alpine`, `hydrogen-alpine3.20`. If you want to display recommendations specifically for a different tag, please re-run the command using the `--tag` flag.

Refresh base image
Rebuild the image using a newer base image version. Updating this may result in breaking changes.
✓ This image version is up to date.

Change base image

At the bottom, there is a dock with various application icons.