Образы Docker: Лучшие практики по безопасности

Авторы
@liran_tal - Node.js Security WG & Developer Advocate из компании Snyk
@omerlh - DevSecOps Engineer из компании Soluto
Переведено
@AnonymousAlmaty – пентестер и специалист по ИБ

https://snyk.io/

https://securixy.kz/

1. Выбирайте минимальные образы

В отчете Snyk о состоянии безопасности открытого исходного кода - 2019 г. обнаружено что образы могут содержать до 580 уязвимостей в системных библиотеках операционной системы.

- ✓ Используйте образы с наименьшим кол-вом библиотек ОС и инструментов для снижения риска
- ✓ Предпочитайте образы на основе alpine вместо полноценных ОС

2. Меньше привилегий

Включите создание выделенного пользователя и выделенной группы в образе Docker; используйте директиву USER в Dockerfile, для запуска приложения с минимально возможным доступом

```
FROM node:10-alpine
USER node
CMD node index.js
```

3. Подписывайте и проверяйте образы

Мы привыкли доверять образу Docker скачанному из интернета не задумываясь о надёжности его источника

- ✓ Используйте Notary для подписи своих образов
- ✓ Проверяйте доверие и целостность подтягиваемых образов

4. Ищи, исправляй и следи за уязвимостями в open source ПО

Регулярно сканируйте образы на уязвимости и сделайте это частью своего CI. Snyk поможет обнаружить уязвимости в системных библиотеках и образах Docker

Просканировать образ Docker помощью этих команд:

```
# fetch the image to be tested so it exists locally
$ docker pull node:10
# scan the image with snyk
$ snyk test --docker node:10 --file=path/to/Dockerfile
```

Включить мониторинг уязвимостей:

```
snyk monitor --docker node:10
```

5. Не забывайте очистить образ от важных данных

Иногда легко случайно забыть в контейнере важную нформацию

- ✓ Используйте многоступенчатые сборки
- ✓ Используйте команду secret
- ✓ Остерегайтесь рекурсивной копии, используйте .dockerignore

6. Используйте фиксированные теги для неизменности

Каждый образ Docker может иметь несколько тегов, которые являются вариантами одних и тех же образов

- ✓ Подробный тег образа, с помощью которого можно отметить версию и операционную систему. Например FROM node:8-alpine
- ✓ Хэш образа чтобы более точно позиционировать версию

7. Используйте **COPY** вместо **ADD**

Произвольные URL, указанные для ADD, могут привести к атакам MITM. Кроме того, ADD неявно распаковывает локальные архивы, которые могут не следует ожидать, что приведет к обходу пути и уязвимостям Zip Slip.
Используйте COPY, если не требуется ADD.

8. Используйте метки данных

Метки с метаданными для образов предоставляют полезную информацию для пользователей.
Добавляйте к ним также информацию о безопасности.
Используйте и сообщайте политику касательно информационной безопасности, добавив файл политики SECURITY.TXT и предоставив эту информацию в метках своих образов.

9. Используйте многоэтапную сборку для безопасных образов

На каждом этапе сборки старайтесь уменьшить её состав до минимально необходимого, это позволит существенно снизить возможную поверхность атаки на образ

10. Используйте линтер

Чтобы избежать распространенных ошибок и учесть рекомендации по передовой практике используйте hadolint