# TABLE OF CONTENTS

Chapter 1. NGC Security Scan Failure Remedies.......................................................... 1
Chapter 1.
NGC SECURITY SCAN FAILURE REMEDIES

NGC Container Registry performs automated security scans on containers pushed to the NGC registry. The scanning tool checks against the content of a dockerfile if provided, or a derived dockerfile based on the docker layer history if the dockerfile is not provided.

The Security Scan tab is displayed on the description page for the specific container and shows the results of the scan. The following are some remedies for select security scan failures:

**CVE Failures**

These failures typically occur for one of two reasons:

- Your container image is built from an older base image which has now been found to have security vulnerabilities.
  
  New CVEs are reported every month, so a base image even a few months old is likely no longer secure.
- Your container is built from a recent base image, but a new CVE has been found since its release.
  
  The NGC scanning tool picks up known CVE updates daily, so an image that passed yesterday may fail today.

In both cases the remedy is usually the same; look for the most recent tag for your base image (**FROM** line in your dockerfile) and rebuild your container.

The following is an example of a base image CVE and the remedy.

**Issue**


**Fix**

Rebuild the image and include the latest package which fixes the identified code flaw.

For example:
Use the latest base image which includes the latest package:

```
FROM ubuntu:19.04
```

or

Include the specific run command to update the old package:

```
apt update && apt install --only-upgrade linux-libc-dev
```

CVE failures can also be triggered by other packages/binaries that you install in your container after the base image. The CVE Failure message should have identified the package or binary that triggered it. Look for a more recent version of that package or binary, update your dockerfile and rebuild your docker image.

**Denied/Exposed Port Failures**

NGC has a list of ports which should not be opened in an NGC Container Image.

An example of a denied port is port 80, the default port for HTTP. HTTP connections (as opposed to HTTPS) are not encrypted and are insecure. Modern browsers will warn against an open HTTP connection and is a bad user experience. Port 443 and HTTPS should be used instead - no warnings will appear and the connection is secure.

The following is the list of denied ports:

- 20 - FTP (there are more secure ways to file transfer)
- 23 - Telnet (recommend using a more secure service than telnet)
- 25 - SMTP (email service isn't a common service to be exposed for NGC containers)
- 80 - HTTP (recommend using https on port 433 instead)
- 115 - FTP (there are more secure ways to file transfer)

For all denied ports, the remedy is to use a secure alternative that provides the same functionality whose default port is not on the list of denied ports.

**Private Key Failures**

The NGC Security Scan identifies any private key crypto files in the image, and fails the scan if it finds them. Private keys are dangerous to leave in a published container image, as they may be used by others to authenticate on private or public services and gain access as an imposter.

The remedy is to remove the private keys and resubmit the container image.

There are cases where a container image includes private test keys to allow users to run tests on the container. These are generally harmless and can be whitelisted if the publisher requests.
Notice

THE INFORMATION IN THIS GUIDE AND ALL OTHER INFORMATION CONTAINED IN NVIDIA DOCUMENTATION REFERENCED IN THIS GUIDE IS PROVIDED “AS IS.” NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE INFORMATION FOR THE PRODUCT, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. Notwithstanding any damages that customer might incur for any reason whatsoever, NVIDIA's aggregate and cumulative liability towards customer for the product described in this guide shall be limited in accordance with the NVIDIA terms and conditions of sale for the product.

THE NVIDIA PRODUCT DESCRIBED IN THIS GUIDE IS NOT FAULT TOLERANT AND IS NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE IN CONNECTION WITH THE DESIGN, CONSTRUCTION, MAINTENANCE, AND/OR OPERATION OF ANY SYSTEM WHERE THE USE OR A FAILURE OF SUCH SYSTEM COULD RESULT IN A SITUATION THAT THREATENS THE SAFETY OF HUMAN LIFE OR SEVERE PHYSICAL HARM OR PROPERTY DAMAGE (INCLUDING, FOR EXAMPLE, USE IN CONNECTION WITH ANY NUCLEAR, AVIONICS, LIFE SUPPORT OR OTHER LIFE CRITICAL APPLICATION). NVIDIA EXPRESSLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR SUCH HIGH RISK USES. NVIDIA SHALL NOT BE LIABLE TO CUSTOMER OR ANY THIRD PARTY, IN WHOLE OR IN PART, FOR ANY CLAIMS OR DAMAGES ARISING FROM SUCH HIGH RISK USES.

NVIDIA makes no representation or warranty that the product described in this guide will be suitable for any specified use without further testing or modification. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer’s sole responsibility to ensure the product is suitable and fit for the application planned by customer and to do the necessary testing for the application in order to avoid a default of the application or the product. Weaknesses in customer’s product designs may affect the quality and reliability of the NVIDIA product and may result in additional or different conditions and/or requirements beyond those contained in this guide. NVIDIA does not accept any liability related to any default, damage, costs or problem which may be based on or attributable to: (i) the use of the NVIDIA product in any manner that is contrary to this guide, or (ii) customer product designs.

Other than the right for customer to use the information in this guide with the product, no other license, either expressed or implied, is hereby granted by NVIDIA under this guide. Reproduction of information in this guide is permissible only if reproduction is approved by NVIDIA in writing, is reproduced without alteration, and is accompanied by all associated conditions, limitations, and notices.

Trademarks

NVIDIA, the NVIDIA logo, and Volta are trademarks and/or registered trademarks of NVIDIA Corporation in the United States and other countries.

Docker and the Docker logo are trademarks or registered trademarks of Docker, Inc. in the United States and/or other countries.

Other company and product names may be trademarks of the respective companies with which they are associated.

Copyright

© 2019 NVIDIA Corporation. All rights reserved.