encryption.CheckAuthorization not working for multi-arch images #69

Closed dimitar-dimitrow opened this issue on Mar 15 · 10 comments

dimitar-dimitrow commented on Mar 15

When a multi-arch index descriptor is provided to the imgcrypt's CheckAuthorization func (e.g. via image.Target()), the library iterates over the manifests it refers to with the cryptoOpUnwrapOnly option set to true to perform a check only. That causes the cycle to stop on the first manifest in the collection as the condition here will always be evaluated to true error-regardless. Additionally, if reading any of the referred manifest's children returns an errdefs.IsNotFound(err), the cycle will exit with a nil error, thus, the authorization check passes incorrectly.
Let's take for example the case where the cycle checks the first manifest in the collection (e.g. for amd64) on an arm/arm64 machine, the children of this manifest are not found since this is not the target platform and they are not pulled -> the authorization check passes incorrectly. This issue is rarely reproducible on an amd64 machine as usually, this is the first manifest in the index descriptor.

stefanberger commented on Mar 15 Contributor

Do you have examples of command lines that you used and ran into this issue?

dimitar-dimitrow commented on Mar 17 • edited Author

```
# ctr-enc -n issue i pull docker.io/library/bash:latest
# ctr-enc -n issue i encrypt --recipient jwe:/home/pi/develop/mypubkey.pem
docker.io/library/bash:latest
# ctr-enc -n issue run -t --key /home/pi/develop/mykey.pem docker.io/library/bash:latest with_key
bash-5.1# exit
exit
# ctr-enc -n issue run -t docker.io/library/bash:latest without_key
bash-5.1# exit
exit
```

Result: The **without_key** container runs without providing the private key.
Expected: Authorization check fails for **without_key**, the container does not run.

stefanberger commented on Mar 17 Contributor

And you are trying this on something other than amd64?

dimitar-dimitrow commented on Mar 17 Author

Yes, on raspberry(armv6l). This issue is rarely reproducible on an amd64 machine as usually, this is the first manifest in the index descriptor. In the case of docker.io/library/bash:latest the first manifest is indeed the amd64 one, so you won't be able to reproduce it on amd64 machine.

stefanberger commented on Mar 17 Contributor

I am running this now on a ppc64 machine. There's a test case in `script/tests/test_encryption.sh` covering exactly this case:

imgcrypt/script/tests/test_encryption.sh
Lines 345 to 359 in `727850f`

```
345         MSG=$(sudo bash -c "$CTR run \
346             --rm \
347             ${ALPINE_ENC} testcontainer1 echo 'Hello world'" 2>&1)
348         if [ $? -eq 0 ]; then
349             MSG=$($CTR snapshot rm testcontainer1 2>&1)
350             failExit 1 "Should not have been able to run a container from encrypted
351         fi
352         MSG=$($CTR snapshot rm testcontainer1 2>&1)
353         MSG=$(sudo bash -c "$CTR run \
354             --gpg-homedir ${GPGHOMEDIR} \
```

Unfortunately it's passing as expected, meaning it refuses to run the encrypted container image without key and runs it when the key is provided.

stefanberger commented on Mar 17 Contributor

So the problem with the test case is that for this image `--all-platforms` were pulled:

imgcrypt/script/tests/test_encryption.sh
Line 166 in `727850f`

```
$CTR images pull ${IMAGE_PULL_CREDS:+--user ${IMAGE_PULL_CREDS}} --all-platforms ${ALP
```

If one doesn't pull `--all-platforms` then this leads to the problem you are seeing.

stefanberger added a commit that referenced this issue on Mar 17

`test: Test running of encrypted image only pulled for local platform` … ✗ b77f7a4

stefanberger mentioned this issue on Mar 17

test: Test running of encrypted image only pulled for local platform #70

Merged

stefanberger added a commit to stefanberger/imgcrypt that referenced this issue on Mar 17

`test: Test running of encrypted image only pulled for local platform` … f978a87

stefanberger added a commit to stefanberger/imgcrypt that referenced this issue on Mar 17

`test: Test running of encrypted image only pulled for local platform` … 8a255bd

stefanberger added a commit to stefanberger/imgcrypt that referenced this issue on Mar 17

`test: Test running of encrypted image only pulled for local platform` … 9ed70ee

stefanberger added a commit to stefanberger/imgcrypt that referenced this issue on Mar 17

`test: Test running of encrypted image only pulled for local platform` … 8094869

stefanberger added a commit to stefanberger/imgcrypt that referenced this issue on Mar 17

`images: Add list of Platforms to CheckAuthorization` … 519cf2e

stefanberger added a commit to stefanberger/imgcrypt that referenced this issue on Mar 17

`test: Test running of encrypted image only pulled for local platform` … 8a81491

stefanberger added a commit to stefanberger/imgcrypt that referenced this issue on Mar 17 `images: Add list of Platforms to CheckAuthorization` … `0749a44`

stefanberger commented on Mar 17 — Contributor

I now have a pending PR. **@dimitar-dimitrow** , maybe you can give it a try.

https://github.com/stefanberger/imgcrypt/tree/fix_issue_69

stefanberger added a commit to stefanberger/imgcrypt that referenced this issue on Mar 17

`test: Test running of encrypted image only pulled for local platform` … `78ebcf0`

stefanberger added a commit to stefanberger/imgcrypt that referenced this issue on Mar 17

`images: Add list of Platforms to CheckAuthorization` … `45d736f`

stefanberger added a commit to stefanberger/imgcrypt that referenced this issue on Mar 17

`images: Add list of Platforms to CheckAuthorization()` … `cfab270`

stefanberger added a commit to stefanberger/imgcrypt that referenced this issue on Mar 18

`test: Test running of encrypted image only pulled for local platform` … `2d51059`

stefanberger added a commit to stefanberger/imgcrypt that referenced this issue on Mar 18

`images: Add list of Platforms to CheckAuthorization()` … `0bbfdb3`

lumjjb pushed a commit that referenced this issue on Mar 21

`test: Test running of encrypted image only pulled for local platform` … `f440058`

lumjjb closed this as completed in `6fdd981` on Mar 21

stefanberger commented on Mar 21 — Contributor

@dimitar-dimitrow Even though the code has been merged already, can you give it a try?

dimitar-dimitrow commented on Mar 21 — Author

@stefanberger Sorry, for the late response, the fix works as expected. Thanks!
Would there be a new version release with this fix soon or should I keep to the snapshot version for now?

stefanberger commented on Mar 23 Contributor

@dimitar-dimitrow I am going to create v1.1.4 once a few more things are merged. I will create a CVE referencing your report. Thanks.

👍 1

GoVulnBot mentioned this issue on Mar 25

x/vulndb: potential Go vuln in github.com/containerd/imgcrypt: CVE-2022-24778
golang/vulndb#412
Closed

jba mentioned this issue on Mar 25

x/vulndb: potential Go vuln in github.com/containerd/imgcrypt: CVE-2022-24778
jba/nested-modules#277
Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants