

[New issue](#)[Jump to bottom](#)segfault in `tf.image.crop_and_resize` when `boxes` contains large value #42129Closed DNXie opened this issue on Aug 7, 2020 · 7 comments · Fixed by #42143

Assignees



Labels

comp:ops

TF 2.2

type:bug

DNXie commented on Aug 7, 2020

Please make sure that this is a bug. As per our [GitHub Policy](#), we only address code/doc bugs, performance issues, feature requests and build/installation issues on GitHub. tag:bug_template

System information

- Have I written custom code (as opposed to using a stock example script provided in TensorFlow): No
- OS Platform and Distribution (e.g., Linux Ubuntu 16.04): Linux Ubuntu 18.04
- Mobile device (e.g. iPhone 8, Pixel 2, Samsung Galaxy) if the issue happens on mobile device: N/A
- TensorFlow installed from (source or binary): binary
- TensorFlow version (use command below): v2.2.0-rc4-8-g2b96f3662b 2.2.0
- Python version: 3.6.9
- Bazel version (if compiling from source): N/A
- GCC/Compiler version (if compiling from source): N/A
- CUDA/cuDNN version: N/A
- GPU model and memory: N/A

Describe the current behavior

`tf.image.crop_and_resize` segfault when there is a very large value in `boxes`. Can also be reproduced in nightly version

Describe the expected behavior

Expect no segfault

Standalone code to reproduce the issue

```
import tensorflow as tf
tf.image.crop_and_resize(image=tf.zeros((2,1,1,1)), boxes=[[1.0e+40, 0,0,0]], box_indices=[1], crop_size=[1,1])
```

Other info / logs Include any logs or source code that would be helpful to diagnose the problem. If including tracebacks, please include the full traceback. Large logs and files should be attached.

Segmentation fault (core dumped)

 DNXie added the `type:bug` label on Aug 7, 2020 google-ml-butler (bot) assigned `ravikyram` on Aug 7, 2020

yongtang mentioned this issue on Aug 7, 2020

Fix segmentation fault in `tf.image.crop_and_resize` when `boxes` is inf or nan #42143Merged

yongtang commented on Aug 7, 2020

Member

Added a PR #42143 for the fix.

 ravikyram added `comp:ops` `TF 2.2` labels on Aug 8, 2020

copybara-service (bot) closed this as completed in #42143 on Oct 19, 2020

google-ml-butler (bot) commented on Oct 19, 2020

Are you satisfied with the resolution of your issue?

Yes

No

copybara-service (bot) pushed a commit that referenced this issue on Oct 20, 2020



Add security advisories for #42105 and #42129. ...

✓ e643795

lvyuqi commented on Apr 9, 2021 • edited

Does this issue affect the 1.15.5 version?
Corresponding CVE Vulnerability [CVE-2020-15266](#)

mihairuseac commented on Apr 11, 2021

Collaborator

Yes, but being low severity and given that patching 1.15 and 2.0 is extremely expensive we no longer patched it.
Recommendation is to update past 2.1

 **github-actions** (bot) mentioned this issue on Jun 22, 2021

Security Alert RasaHQ/rasa#8638

 Closed

mgmm13 commented on Sep 2, 2021

Hello, is there any chance that vulnerability fix will be applied in versions like 2.3.4?

 2

mihairuseac commented on Sep 2, 2021

Collaborator

Hi. Not in 2.3.4, as the 2.3.x has reached end of life.
It is already included in 2.4.0 and later

mgmm13 commented on Sep 2, 2021

@mihairuseac noted on this, thank you for the feedback.

Assignees

 ravikyram

Labels

comp:ops TF 2.2 type:bug

Projects


None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 Fix segmentation fault in tf.image.crop_and_resize when boxes is inf or nan
yongtang/tensorflow

6 participants

