Division by zero in `Conv3D`

Low **mihaimaruseac** published **GHSA-772p-x54p-hjrv** 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

A malicious user could trigger a division by 0 in `Conv3D` implementation:

```
import tensorflow as tf

input_tensor = tf.constant([], shape=[0, 0, 0, 0, 0], dtype=tf.float32)
filter_tensor = tf.constant([], shape=[0, 0, 0, 0, 0], dtype=tf.float32)

tf.raw_ops.Conv3D(input=input_tensor, filter=filter_tensor, strides=[1, 56, 56, 56, 1], padding='VALID', data_format='NDHWC', dilations=[1, 1, 1, 23, 1])
```

The implementation does a modulo operation based on user controlled input:

```
  const int64 out_depth = filter.dim_size(4);
  OP_REQUIRES(context, in_depth % filter_depth == 0, ...);
```

Thus, when `filter` has a 0 as the fifth element, this results in a division by 0.

Additionally, if the shape of the two tensors is not valid, an Eigen assertion can be triggered, resulting in a program crash:

```
import tensorflow as tf

input_tensor = tf.constant([], shape=[2, 2, 2, 2, 0], dtype=tf.float32)
filter_tensor = tf.constant([], shape=[0, 0, 2, 6, 2], dtype=tf.float32)

tf.raw_ops.Conv3D(input=input_tensor, filter=filter_tensor, strides=[1, 56, 39, 34, 1], padding='VALID', data_format='NDHWC', dilations=[1, 1, 1, 1, 1])
```

The shape of the two tensors must follow the constraints specified in the op description.

Patches

We have patched the issue in GitHub commit 799f835a3dfa00a4d852defa29b15841eea9d64f.

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-2021-29517

Weaknesses

No CWEs