Invalid validation in `QuantizeAndDequantizeV2`

Low **mihaimaruseac** published **GHSA-mq5c-prh3-3f3h** 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

The validation in `tf.raw_ops.QuantizeAndDequantizeV2` allows invalid values for `axis` argument:

```
import tensorflow as tf

input_tensor = tf.constant([0.0], shape=[1], dtype=float)
input_min = tf.constant(-10.0)
input_max = tf.constant(-10.0)

tf.raw_ops.QuantizeAndDequantizeV2(
  input=input_tensor, input_min=input_min, input_max=input_max,
  signed_input=False, num_bits=1, range_given=False, round_mode='HALF_TO_EVEN',
  narrow_range=False, axis=-2)
```

The validation uses `||` to mix two different conditions:

```
OP_REQUIRES(ctx,
  (axis_ == -1 || axis_ < input.shape().dims()),
  errors::InvalidArgument(...));
```

If `axis_ < -1` the condition in `OP_REQUIRES` will still be true, but this value of `axis_` results in heap underflow. This allows attackers to read/write to other data on the heap.

Patches

We have patched the issue in GitHub commit c5b0d5f8ac19888e46ca14b0e27562e7fbbee9a9.

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-2021-29610

Weaknesses

No CWEs