Missing validation crashes `QuantizeAndDequantizeV4Grad`

Low **mihaimaruseac** published **GHSA-h2wq-prv9-2f56** on May 17

Package

tensorflow, tensorflow-cpu, tensorflow-gpu (pip)

Affected versions	Patched versions
< 2.9.0	2.6.4, 2.7.2, 2.8.1, 2.9.0

Description

Impact

The implementation of `tf.raw_ops.QuantizeAndDequantizeV4Grad` does not fully validate the input arguments. This results in a `CHECK` -failure which can be used to trigger a denial of service attack:

```
import tensorflow as tf

tf.raw_ops.QuantizeAndDequantizeV4Grad(
  gradients=tf.constant(1, shape=[2,2], dtype=tf.float64),
  input=tf.constant(1, shape=[2,2], dtype=tf.float64),
  input_min=tf.constant([], shape=[0], dtype=tf.float64),
  input_max=tf.constant(-10, shape=[], dtype=tf.float64),
  axis=-1)
```

The code assumes `input_min` and `input_max` are scalars but there is no validation for this.

Patches

We have patched the issue in GitHub commit 098e7762d909bac47ce1dbabe6dfd06294cb9d58.

The fix will be included in TensorFlow 2.9.0. We will also cherrypick this commit on TensorFlow 2.8.1, TensorFlow 2.7.2, and TensorFlow 2.6.4, 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 Neophytos Christou from Secure Systems Lab at Brown University.

Severity

Low

CVE ID

CVE-2022-29192

Weaknesses

No CWEs