Division by 0 in `MaxPoolGradWithArgmax`

Low **mihaimaruseac** published **GHSA-9vpm-rcf4-9wqw** 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 implementation of `tf.raw_ops.MaxPoolGradWithArgmax` is vulnerable to a division by 0:

```
import tensorflow as tf

input = tf.constant([], shape=[0, 0, 0, 0], dtype=tf.float32)
grad = tf.constant([], shape=[0, 0, 0, 0], dtype=tf.float32)
argmax = tf.constant([], shape=[0], dtype=tf.int64)
ksize = [1, 1, 1, 1]
strides = [1, 1, 1, 1]

tf.raw_ops.MaxPoolGradWithArgmax(
  input=input, grad=grad, argmax=argmax, ksize=ksize, strides=strides,
  padding='SAME', include_batch_in_index=False)
```

The implementation fails to validate that the batch dimension of the tensor is non-zero, before dividing by this quantity.

Patches

We have patched the issue in GitHub commit 376c352a37ce5a68b721406dc7e77ac4b6cf483d.

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-2021-29573

Weaknesses

No CWEs