Heap buffer overflow in `AvgPool3DGrad`

Low **mihaimaruseac** published **GHSA-v6r6-84gr-92rm** 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.AvgPool3DGrad` is vulnerable to a heap buffer overflow:

```
import tensorflow as tf

orig_input_shape = tf.constant([10, 6, 3, 7, 7], shape=[5], dtype=tf.int32)
grad = tf.constant([0.01, 0, 0], shape=[3, 1, 1, 1, 1], dtype=tf.float32)
ksize = [1, 1, 1, 1, 1]
strides = [1, 1, 1, 1, 1]
padding = "SAME"

tf.raw_ops.AvgPool3DGrad(
  orig_input_shape=orig_input_shape, grad=grad, ksize=ksize, strides=strides,
  padding=padding)
```

The implementation assumes that the `orig_input_shape` and `grad` tensors have similar first and last dimensions but does not check that this assumption is validated.

Patches

We have patched the issue in GitHub commit 6fc9141f42f6a72180ecd24021c3e6b36165fe0d.

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-2021-29577

Weaknesses

No CWEs