Memory corruption in `DrawBoundingBoxesV2`

Moderate mihaimaruseac published GHSA-whr9-vfh2-7hm6 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.MaxPoolGradWithArgmax` can cause reads outside of bounds of heap allocated data if attacker supplies specially crafted inputs:

```
import tensorflow as tf

images = tf.fill([10, 96, 0, 1], 0.)
boxes = tf.fill([10, 53, 0], 0.)
colors = tf.fill([0, 1], 0.)

tf.raw_ops.DrawBoundingBoxesV2(images=images, boxes=boxes, colors=colors)
```

The implementation assumes that the last element of `boxes` input is 4, as required by the op. Since this is not checked attackers passing values less than 4 can write outside of bounds of heap allocated objects and cause memory corruption:

```
const auto tboxes = boxes.tensor<T, 3>();
for (int64 bb = 0; bb < num_boxes; ++bb) {
  ...
  const int64 min_box_row = static_cast<float>(tboxes(b, bb, 0)) * (height - 1);
  const int64 max_box_row = static_cast<float>(tboxes(b, bb, 2)) * (height - 1);
  const int64 min_box_col = static_cast<float>(tboxes(b, bb, 1)) * (width - 1);
  const int64 max_box_col = static_cast<float>(tboxes(b, bb, 3)) * (width - 1);
  ...
}
```

If the last dimension in `boxes` is less than 4, accesses similar to `tboxes(b, bb, 3)` will access data outside of bounds. Further during code execution there are also writes to these indices.

Patches

We have patched the issue in GitHub commit 79865b542f9ffdc9caeb255631f7c56f1d4b6517.

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

Moderate

CVE ID

CVE-2021-29571

Weaknesses

No CWEs