`CHECK`-fail in `DrawBoundingBoxes`

Low **mihaimaruseac** published **GHSA-393f-2jr3-cp69** 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 trigger a denial of service via a `CHECK` failure by passing an empty image to `tf.raw_ops.DrawBoundingBoxes`:

```
import tensorflow as tf

images = tf.fill([53, 0, 48, 1], 0.)
boxes = tf.fill([53, 31, 4], 0.)
boxes = tf.Variable(boxes)
boxes[0, 0, 0].assign(3.90621)
tf.raw_ops.DrawBoundingBoxes(images=images, boxes=boxes)
```

This is because the implementation uses `CHECK_*` assertions instead of `OP_REQUIRES` to validate user controlled inputs. Whereas `OP_REQUIRES` allows returning an error condition back to the user, the `CHECK_*` macros result in a crash if the condition is false, similar to `assert`.

```
const int64 max_box_row_clamp = std::min<int64>(max_box_row, height - 1);
...
CHECK_GE(max_box_row_clamp, 0);
```

In this case, `height` is 0 from the `images` input. This results in `max_box_row_clamp` being negative and the assertion being falsified, followed by aborting program execution.

Patches

We have patched the issue in GitHub commit b432a38fe0e1b4b904a6c222cbce794c39703e87.

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-2021-29533

Weaknesses

No CWEs