Missing validation causes denial of service via `UnsortedSegmentJoin`

Low **mihaimaruseac** published **GHSA-hrg5-737c-2p56** on May 17

Package

tensorflow, tensorflow-cpu, tensorflow-gpu (pip)

Affected versions	Patched versions
< 2.9.0	2.6.4, 2.7.2, 2.8.1, 2.9.0

Description

Impact

The implementation of `tf.raw_ops.UnsortedSegmentJoin` does not fully validate the input arguments. This results in a `CHECK` -failure which can be used to trigger a denial of service attack:

```
import tensorflow as tf

tf.raw_ops.UnsortedSegmentJoin(
  inputs=tf.constant("this", shape=[12], dtype=tf.string),
  segment_ids=tf.constant(0, shape=[12], dtype=tf.int64),
  num_segments=tf.constant(0, shape=[12], dtype=tf.int64))
```

The code assumes `num_segments` is a scalar but there is no validation for this before accessing its value:

```
const Tensor& num_segments_tensor = context->input(2);
OP_REQUIRES(context, num_segments_tensor.NumElements() != 0,
            errors::InvalidArgument("Number of segments cannot be empty."));
auto num_segments = num_segments_tensor.scalar<NUM_SEGMENTS_TYPE>()();
```

Patches

We have patched the issue in GitHub commit 13d38a07ce9143e044aa737cfd7bb759d0e9b400.

The fix will be included in TensorFlow 2.9.0. We will also cherrypick this commit on TensorFlow 2.8.1, TensorFlow 2.7.2, and TensorFlow 2.6.4, 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 Neophytos Christou from Secure Systems Lab at Brown University.

Severity

Low

CVE ID

CVE-2022-29197

Weaknesses

No CWEs