Null pointer dereference via invalid Ragged Tensors

Low **mihaimaruseac** published **GHSA-84mw-34w6-2q43** 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

Calling `tf.raw_ops.RaggedTensorToVariant` with arguments specifying an invalid ragged tensor results in a null pointer dereference:

```
import tensorflow as tf

input_tensor = tf.constant([], shape=[0, 0, 0, 0, 0], dtype=tf.float32)
filter_tensor = tf.constant([], shape=[0, 0, 0, 0, 0], dtype=tf.float32)

tf.raw_ops.Conv3D(input=input_tensor, filter=filter_tensor, strides=[1, 56, 56, 56, 1], padding='VALID', data_format='NDHWC', dilations=[1, 1, 1, 23, 1])
```

```
import tensorflow as tf

input_tensor = tf.constant([], shape=[2, 2, 2, 2, 0], dtype=tf.float32)
filter_tensor = tf.constant([], shape=[0, 0, 2, 6, 2], dtype=tf.float32)

tf.raw_ops.Conv3D(input=input_tensor, filter=filter_tensor, strides=[1, 56, 39, 34, 1], padding='VALID', data_format='NDHWC', dilations=[1, 1, 1, 1, 1])
```

The implementation of `RaggedTensorToVariant` operations does not validate that the ragged tensor argument is non-empty:

```
  int ragged_rank = batched_ragged.ragged_rank();
  auto batched_splits_top_vec = batched_ragged.splits(0).vec<SPLIT_TYPE>();
```

Since `batched_ragged` contains no elements, `batched_ragged.splits` is a null vector, thus `batched_ragged.splits(0)` will result in dereferencing `nullptr`.

Patches

We have patched the issue in GitHub commit b055b9c474cd376259dde8779908f9eeaf097d93.

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-2021-29516

Weaknesses

No CWEs