Abort due to invalid splits in RaggedCountSparseOutput

Moderate **mihaimaruseac** published **GHSA-x5cp-9pcf-pp3h** on Sep 24, 2020

Package

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

Affected versions	Patched versions
2.3.0	2.3.1

Description

Impact

The `RaggedCountSparseOutput` does not validate that the input arguments form a valid ragged tensor. In particular, there is no validation that the `splits` tensor has the minimum required number of elements. Code uses this quantity to initialize a different data structure:

tensorflow/tensorflow/core/kernels/count_ops.cc
Lines 241 to 244 in `0e68f4d`

```
241     int num_batches = splits.NumElements() - 1;
242     int num_values = values.NumElements();
243
244     auto per_batch_counts = BatchedMap<W>(num_batches);
```

Since `BatchedMap` is equivalent to a vector, it needs to have at least one element to not be `nullptr`. If user passes a `splits` tensor that is empty or has exactly one element, we get a `SIGABRT` signal raised by the operating system.

Patches

We have patched the issue in `3cbb917` and will release a patch release.

We recommend users to upgrade to TensorFlow 2.3.1.

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 is a variant of GHSA-p5f8-gfw5-33w4

Severity

Moderate

CVE ID

CVE-2020-15199

Weaknesses

No CWEs